EXHIBIT B

BITC•IN
MINING
HANDBOOK

Explore the fundamentals
of bitcoin mining

Author: **DANIEL FRUMKIN**
Foreword: **MARTY BENT**

BRAIINS Insights

BRAIINS INSIGHTS:
BITCOIN MINING HANDBOOK

Written by
Daniel Frumkin of Braiins

With contributors:
**Dave White, Tyler Cohoon,
Magdalena Gronowska (Crypto Mags),
Zack Voell, Matyas Kuchar**

Foreword by
Marty Bent

BRAIINS Insights

BRA\\NS Insights
Bitcoin Mining Handbook

Written by: Daniel Frumkin
Contributors: Dave White, Tyler Cohoon, Magdalena (Mags) Gronowska, Zack Voell, Matyas Kuchar

Editors: Daniel Frumkin, Zach Voell, Jáchym Černý
Cover design: Jiří Chlebus
Design consulting: Robert Blecha
Illustrations: Tomáš Nadymáček
Typesetting: Sabina Heyová
Marketing strategy: Kristian Csepcsar

BRAIINS

OPTIMIZING YOUR BITCOIN MINING OPERATIONS
With a full-stack solution including ASIC autotuning firmware, farm management, and the oldest mining pool still in operation.

BRAIINS OS +

FARM Proxy   STRATUM V2

BRAIINS POOL

Formerly **Slush Pool**

BONUS: Our good friends at Bitrefill make it easy to live on a bitcoin standard. They are offering a one-time* 10% satsback (That's not a typo, 1-0-%!!!) on ANY PURCHASE by ANY USER. Simply enter code "BRAIINS" at checkout.

*This is a limited time offer - an ongoing deal will replace it and can be found by downloading the updated version of the Bitcoin Mining Handbook.

Contents

Foreword from Marty Bent

Bitcoin mining is an industry built on ruthless competition. Economic actors from across the world are engaged in a never ending quest to provide the bitcoin network with the essential service of adding blocks of valid transactions to the distributed ledger and being rewarded in bitcoin for their work. This quest involves a mad dash to acquire energy assets, power purchase agreements, capital intensive infrastructure, and specialized computers all in the hopes of building an operation that produces bitcoin at the lowest cost possible. The economic actors competing with each other operate on an extremely wide spectrum due to the permissionless nature of bitcoin and, by extension, bitcoin mining.

Anyone who is so motivated can acquire a bitcoin-specific ASIC and begin contributing to the network. This is why the mining industry includes everyone from your local cypherpunk running a single ASIC in his basement to increase the size of his KYC-free stack to publicly traded corporations with multi-hundred megawatt facilities and quarterly earnings reports that are hawked by equities analysts from the largest financial institutions in the world. No matter the size of the operator, bitcoin mining is a game that one can work to improve over time. One of the best ways to improve your game is to make sure you are leveraging the best tools at your disposal.

Over the course of the last decade, the team at Braiins has been working diligently to bring bitcoin miners of any size the tools that enable them to be smarter and more profitable operators.

Braiins Pool (the now "formerly", Slush Pool) was launched in 2010 so that smaller miners could pool their hashrate together to reduce the variability of their payouts. Helping create more certainty around

revenue streams that has allowed smaller miners to keep playing the game. Many pools have come and gone since 2010, yet Braiins Pool has remained the stalwart of the industry. With the pool well established and miners continuing their quest to become as efficient and profitable as possible, Braiins brought their Braiins OS+ autotuning firmware to market. Providing miners with the option to replace their stock firmware, which was sometimes found to be riddled with backdoors, with a custom firmware that would enable them to run more efficiently and manage their operations more granularly. Increasing the profitability and lifespan of precious ASICs as a result.

The mining pool technology pioneered in Braiins Pool and the autotuning firmware that the Braiins team have brought to market are two of the most profound tools that have been made available to miners in the nascent stage of the bitcoin mining industry that we find ourselves in today. However, the value-add to miners does not stop there. Pooling technology and firmware are cool, but what's cooler is being able to leverage them to the best of your abilities. That means being equipped with knowledge that produces better business decisions. Do not fear. Braiins has you covered on that front with their blog, which will get you acquainted with the basics of mining as well as the latest trends.

Even better, they built a Braiins Insights dashboard that provides anyone who is interested with all of the pertinent details of the state of the mining industry at any given point in time. Network hashrate, difficulty, pool distribution, hashprice, hashvalue, ASIC model profitability, the state of the fee market, and daily revenue for all miners on the network. It's all there in one spot. Waiting for you to leverage it to make the best decisions you can for your mining operation, no matter how small or large. As the ruthless competition becomes more... ruthless, being able to use this information effectively will be what separates you and those you are competing with.

If you are going to read a bitcoin mining handbook it is probably best that it be written by a team with the extensive experience and

knowledge that the Braiins team brings with it. They've accumulated a decade of proof-of-work and are here to share what they've learned with you. (Did you really think I was going to get through this without a cheesy mining pun?)

I have been an admirer and user of Braiins' products for many years. I consider myself extremely lucky to have Braiins as an official partner of TFTC. To think that they feel comfortable aligning their prestigious brand with mine brings me much joy. Needless to say, I am honored to be writing the foreword to this handbook.

Now go forth and educate yourself. You are in good hands.

Final thought...

Swimming pools are the worst.

Preface

For all the criticisms that bitcoin mining receives from the public, very few actually understand how it works and the monetary features of bitcoin that it uniquely enables. Proof of work connects bitcoin to the physical world through a fundamental part of life: energy. The expenditure of energy in bitcoin mining is what gives us indisputable truth about the state of the ledger and what makes it immutable over time. The only way to change even one transaction in bitcoin's history is to do more work than all of the miners combined in the entire network have done since that transaction was first added to the blockchain. In bitcoin, unlike in the fiat system and the vast majority of alternative cryptocurrency projects, there is no such thing as a free lunch. All that matters is doing the work.

In 1921, the New York Tribune ran a piece titled, *Ford Would Replace Gold With Energy Currency and Stop Wars*, in which Henry Ford laid out the case that a currency backed by energy would reduce the power of bankers and put an end to much international conflict. As Ford stated,

"With the international bankers, the fostering, starting and fighting of a war is nothing more nor less than creating an active market for money—a business transaction. ...No matter who loses the war, there have been a great many loans—the gold system always wins."

New York

First to Last — the Truth: Nev

412   (Copyright, 1921,   SUNDAY, DECEMBER 4, 192
New York Tribune Inc.)

Ford Would Replace Gold With Energy Currency and Stop Wars

Declares if Government Will Give Him Muscle Shoals Plant He Can Demonstrate Success of Plan to Substitute Natural Wealth as Basis of World's Money

FLORENCE, Ala., Dec. 3.—Henry Ford and Thomas A. Edison arrived here to-day to inspect the Muscle Shoals nitrate plant, which the Detroit automobile manufacturer proposes to take over from the government, and almost immediately Mr. Ford declared the purpose of his vast new project. It is not to make money, or, primarily, to stimulate the employment of a million men now idle, or to make the South an industrial center. His purpose, he said, is to end all wars forever.

Henry Ford, by building the world's greatest power plant here on the Tennessee River, expects to eliminate gold as the basis of world wealth and substitute for it something different—

bankers who td-day control the bulk of the world's gold supply. No matter to what country they as individuals claim allegiance, they all play the same game to keep the gold they have in their own hands and to get just as much more as possible.

"With the international bankers fostering, starting and fighting of a war is nothing more nor less than creating an active market for money—a business transaction. If the different countries of the international groups are at war—that makes no difference. No matter who loses the war there have been a great many loans—the gold system always wins. The young men from eighteen to thirty fight the war and are maimed or killed, the internationalists are safe and prosperous.

"Ten years ago I said I intended to put every ounce of brains and energy

Craig Urges $10,000,000 Education Cut

Slash Into School Funds Suggested to Aldermen to Obtain Reduction in $350,516,524 Budget

State Called Upon To Make Up Deficit

No Other City Department To Be Touched in Plan to Equalize Taxation

Comptroller Charles L. Craig yesterday sent a letter to Alderman Frank

Although the gold standard began to crumble around the time of Ford's comments, it was replaced by a credit-based fiat system which moved in the opposite direction that Ford desired by giving even more power to bankers and seeing the financial sector grow to consume an ever-larger portion of GDP. Bitcoin is the realization of Ford's now century-old vision of a money and a monetary system based on energy, free of the control of bankers, governments, and any other centralized groups. Proof of work is the foundation of it all.

We hope that this collection of articles from our blog will help you and all those you share it with to understand bitcoin mining more deeply and to appreciate its importance in establishing a politically neutral, permissionless, and efficient monetary system for the entire world.

x

BITCOIN MINING BASICS

You'll often hear in the bitcoin community that the fiat system is based on trust in people and governments while bitcoin is based on trust in math. This is true, but it frequently leads to misconceptions about mining for bitcoiners and non-bitcoiners alike. Are miners solving super complicated math problems? Well, not really—not in the way that it's usually interpreted, anyway.

Every modern mining machine today performs trillions of hash computations per second (terahashes / second). Each of these is a complex calculation that would take humans a very long time, but for computers it is not so hard—thus the trillions per second that they can do.

In this section, we clear up some misconceptions about how bitcoin mining really works and then dive deeper into the why of mining. What benefits does mining provide, why can't we just have nodes that don't consume lots of energy (i.e. proof of stake) for consensus, what are the differences between nodes and miners in bitcoin, and so on. We finish the section with an analysis of the hypothetical cost to 51% attack bitcoin that explains why money is hardly the biggest obstacle in pulling off any attacks.

It's quite difficult to counter FUD about bitcoin mining without understanding how it works and what differentiates it from alternatives like proof of stake. By the end of this section, you should be well-equipped to discuss the merits of proof of work with all the curious learners as well as the naysayers out there.

Bitcoin Mining is NOT Solving Complex Math Problems [Beginner's Guide]

Bitcoin mining and difficulty adjustments explained in non-technical terms using a simple dice analogy.

Most people misunderstand what bitcoin miners actually do, and as a result they don't fully grasp the level of security provided by bitcoin's hashrate. In this article, we'll explain proof of work in a non-technical way so that you'll be able to counter the misinformation about supercomputers and quantum computers attacking the Bitcoin network in the future. Simply put, mining is a lottery to create new blocks in the Bitcoin blockchain. There are two main purposes for mining:
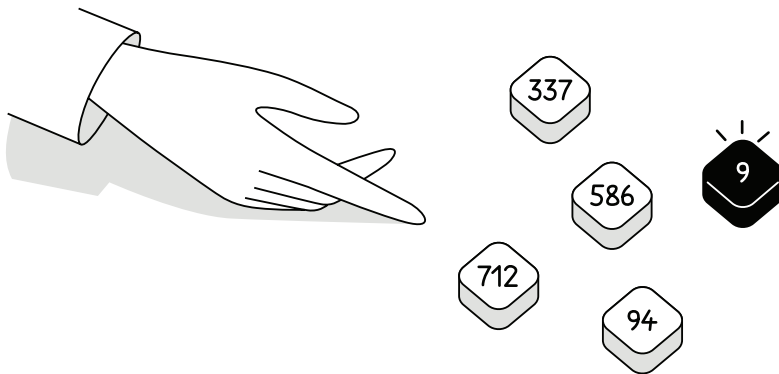
1. To permanently add transactions to the blockchain without the permission of any entity.

2. To fairly distribute the 21 million bitcoin supply by rewarding new coins to miners who spend real world resources (i.e. electricity) to secure the network.

To understand what is actually happening in this lottery system, let's look at a simple analogy where every Bitcoin hash is equivalent to a dice roll.

LUCK, GAMBLING, AND SHA256

Imagine that miners in the Bitcoin Network are all individuals gambling at a casino. In this example, each of these gamblers have a 1000 sided dice. They roll their die as quickly as possible, trying to get a number less than 10. Statistically, this may take a very long time, but as more gamblers join the game, the time it takes to hit a number less than 10 gets reduced. In short, more gamblers equals quicker rounds. Once somebody successfully rolls a number less than 10, all gamblers

12

at the table can look down and verify the number. This lucky gambler takes the prize money and the next round begins.
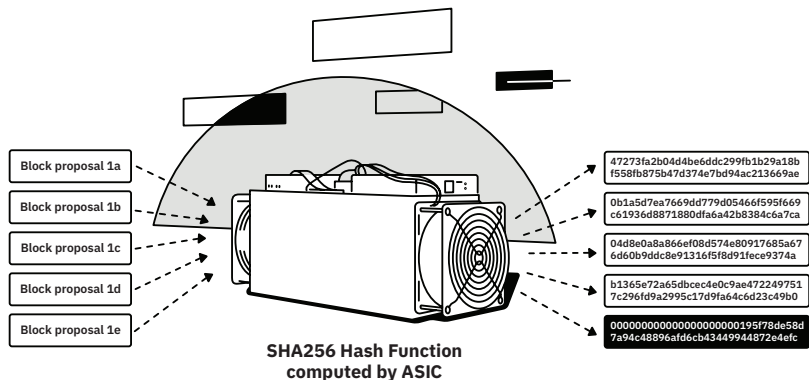
The lucky gambler rolls a number below 10

Ultimately, the process of mining bitcoin is very similar. All miners on the network are using Application Specific Integrated Circuits (ASICs), which are specialized computers designed to compute hashes as quickly as possible. To "compute a hash" simply means plugging any random input into a mathematical function and producing an output.

More hashes per second (i.e. higher hashrate) is equivalent to more dice rolls per second, and thus a greater probability of success. Miners propose a potential Bitcoin block of transactions, and use this for an input. The block is plugged into the SHA256 hash function which yields a fixed-sized output, known as a hash. A single hash can be computed in less than a millisecond, as it involves no complex math (by computer standards, anyway).

If the hash value is lower than the Bitcoin Network difficulty, then the miner who proposed the block wins. If not, then the miner continues trying by computing more hashes. The successful miner's block is then added to the blockchain, the miner is rewarded with newly issued bitcoin for their work, and the "next round" begins.

13

Block proposal 1a	47273fa2b04d4be6ddc299fb1b29a18bf558fb875b47d374e7bd94ac213669ae
Block proposal 1b	0b1a5d7ea7669dd779d05466f595f669c61936d8871880dfa6a42b8384c6a7ca
Block proposal 1c	04d8e0a8a866ef08d574e80917685a676d60b9ddc8e91316f5f8d91fece9374a
Block proposal 1d	b1365e72a65dbcec4e0c9ae4722497517c296fd9a2995c17d9fa64c6d23c49b0
Block proposal 1e	0000000000000000000195f78de58d7a94c48896afd6cb43449944872e4efc

**SHA256 Hash Function
computed by ASIC**

The winning hash has many leading zeroes
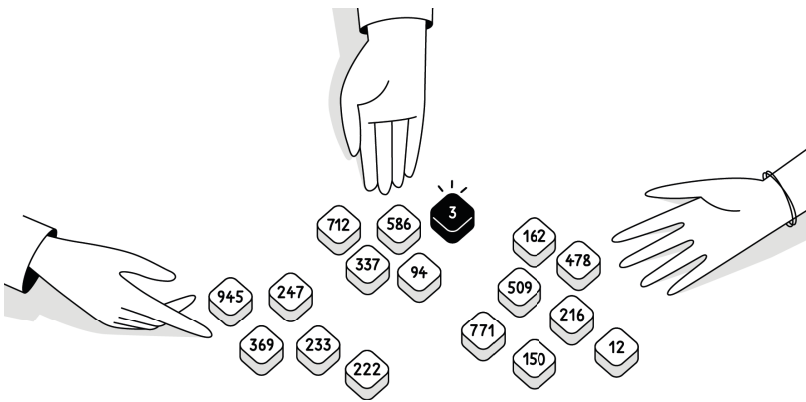
ASICS VS SUPERCOMPUTERS

Assigning the most powerful supercomputer to mine bitcoin would be comparable to hiring a grandmaster chess player to move a pile of bricks by hand. The job would get done eventually but the chess player is much better at thinking and playing chess than exerting energy to repetitively move bricks.

Likewise, combining the computing power of the most powerful supercomputers in the world and using them to mine bitcoin would essentially be pointless when compared to the ASIC machines used today. ASICs are designed to do one thing as quickly and efficiently as possible, whereas a supercomputer is designed to do complicated tasks or math problems. Since Bitcoin mining is a lottery based on random trial and error rather than complex math, specialization (ASICs) beats general excellence (supercomputers) everytime.

NETWORK DIFFICULTY AND 10-MINUTE BLOCK TIMES

Now that you understand the randomness of miners finding a block, it is important to understand block times and difficulty. In our gambling

example, imagine that anybody can join or leave the table at any time. If one person is rolling a 1000 sided die trying to get less than a 10 it will take them an average of 10 minutes to hit that number. Sometimes they'll hit in 1 minute, other times it might take them 30. If a new person steps up to the table and starts rolling, collectively it will take them an average of 5 minutes for somebody to win the round. If 20 people step up to the table, this time is significantly shortened. In order to keep the game interesting we want to average a winner every 10 minutes. To do this, we can simply adjust the dice target. As additional gamblers step up to the table, the rules will change (i.e., gamblers must now roll a number less than 5 to win) so that the average remains 10 minutes per round. As more gamblers join, the casino makes winning harder. If gamblers leave, they make it easier.

Now only rolls below "5" are winning

This is exactly how the Bitcoin network regulates mining to maintain a steady issuance schedule of new BTC. Miners compute hashes below the target difficulty every 10 minutes on average. Every 2016 blocks (~2 weeks) the average for those blocks is calculated and the difficulty is adjusted to bring block times back to 10 minutes. If more miners join the network in this ~2 week period, the hashrate and difficulty will increase as a result.

15

Note: Nobody knows exactly why these arbitrary numbers were chosen. That said, it's important that 10 minutes is long enough for miners and nodes to pass information around the world without internet speeds causing significant issues, and 2016 blocks is long enough to get a statistically accurate block time needed for the difficulty adjustment.

TRULY TRANSPARENT SUPPLY

The difficulty adjustments described above make Bitcoin the only asset with a truly fixed and known supply schedule. Since inception, we've known two things:

1. There will never be more than 21 million coins.

2. Every 10 minutes more bitcoin is newly issued as we approach that 21 million number.

In every other industry, (gold, auto, or even sandwich bags) the supply fluctuates based on demand. If demand increases for automobiles, then the manufacturer can increase production to match the demand. In Bitcoin, supply is locked in and cannot change, therefore demand and price are tied more closely than any other industry or asset classes. This sounds very cut and dry, but it gets interesting when you try to understand what miners do with their newly issued coins and the impact this has on the market.

MINING IN 2021

At the time of writing this article (04/14/2021), more than 89% of the total 21 million coins have been issued. Currently 6.25 BTC are added to the supply every block.

On this date, the price has increased dramatically compared to the growth in network hashrate. This means that price is going up faster than mining difficulty, and thus the revenue that miners are earning

16

per unit of hashpower (i.e. BTC/TH) is increasing. Additionally, there is a semiconductor shortage that is making it difficult for mining manufacturers to secure chips and make new ASICs. This combination of factors is making it so that even old generation ASICs can profitably mine bitcoin, which is great for all miners including hobbyists and home miners who cannot easily secure competitive electricity costs. Pairing this with our Braiins OS+ firmware, one can further increase the profitability of older ASICs like the Antminer S9 by optimizing performance and efficiency.

On the Merits of Proof of Work

Overviewing bitcoin's proof of work mining from an engineering perspective, with historical context and comparisons of the tradeoffs with proof of stake.

Amidst the concern over bitcoin mining's energy usage, and the increased use of proof of stake (PoS) as a consensus mechanism for most new blockchains, popular rhetoric often concludes that proof of work (PoW) is outdated and wasteful. This position, however, is misguided as it usually stems from a lack of understanding for why proof of work exists, and the reasons it was designed to behave the way it does. This article will quickly explain why proof of work is a significant feature of the bitcoin protocol, and how it is unique from the numerous proof of stake networks that seem to emerge on an almost monthly basis.

HISTORICAL CONTEXT

It may be surprising, but proof of work's first application was not in solving for state consensus in a global monetary network. It has much humbler roots, where it was first applied to counteract spam. As Adam Back explains in this 2014 interview (Let's Talk Bitcoin - Episode #77) he first devised the scheme as a way to combat spam in Usenet and remailers, where spammers would abuse these forums by posting reams of irrelevant and useless junk. As the cost to send messages was virtually zero, the economics were such that it was profitable to send spam to potentially reach millions of computers. Adam's insight was to require a user's CPU to perform a bit of work, in order to assign a cost to be able to send a message on the network.

18

His design set incentives such that the cost to normal users would not be prohibitive, but did not scale for users that were abusing the resources. He applied his knowledge of a phenomenon known as "birthday collisions," adapted for a computer, wherein the computer would perform SHA1 hashes on an input until it found the desired output (the "collision"). These collisions could be estimated to occur after a predictable duration, on average. Each collision or event would mint a digital "stamp" that could be used as proof of postage paid, which represented the small amount of electricity and computing power required to produce the stamp.

This was the genesis of something he called Hashcash, and from the description provided, its relevance to bitcoin should be immediately apparent—the algorithm is essentially the same, and these stamps are the great ancestors of bitcoin itself.

BITCOIN AS A COMMUNICATION PROTOCOL

Through Adam's contributions to the Cypherpunks Mailing List, the idea to use hashcash and proof of work in a digital payments network emerged. **In retrospect, it should be clear why proof of work fits so perfectly here: the bitcoin protocol is itself a giant communication network.**

The bitcoin blockchain has a ledger, composed of blocks, which comprises the data of the network. A block has finite space, and the system is designed to create a new block roughly every ten minutes. Given the constraints, the communication protocol has a natural limit on the rate of transactions per minute.
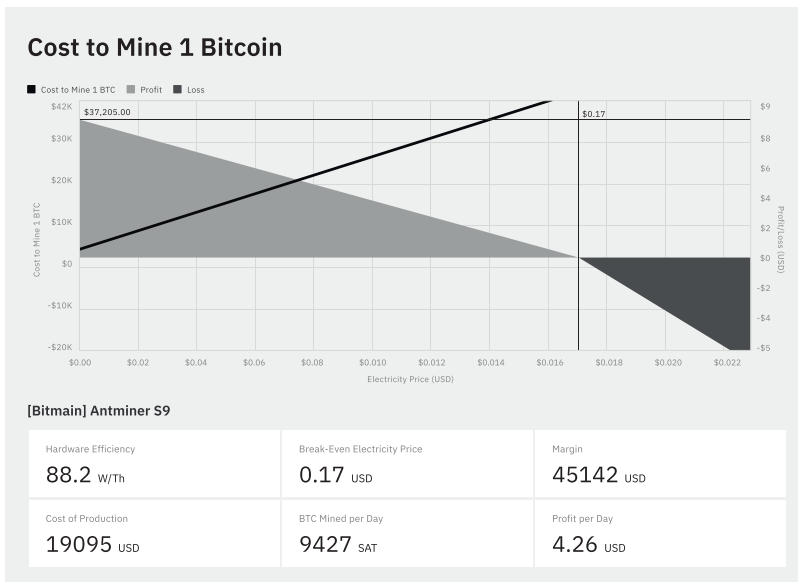
Consequently, if the cost to write to blocks were zero, then anyone who wanted to fill the network with bogus transactions could do so, and effectively prevent legitimate transactions from getting through. This would be a method of censoring the network, through a denial of service attack.

19

Additionally, if another consensus method were used, such as one address one vote, then these spammers could just create a large number of accounts to unduly influence the arrangement of transactions, and which ones get included in a block — all at essentially zero cost. This is what's known as a Sybil attack. Fortunately, writing to the bitcoin ledger isn't free. Because of proof of work, miners must complete trillions of hashes to find a block, which expends energy, and thereby costs money to produce. Measured in time, block space—bandwidth, essentially—inherits a price to prevent abuse of the network, and to ensure that legitimate users are able to participate. Miners are rewarded for their service by the incentive of the block reward, in addition to fees paid by the users to get their transactions included in a block.

ELECTRICITY AND BITCOIN

Electricity is the highest grade energy available, and it is the currency of a digital world. When a block is secured, it can be measured in this base currency as the number of Joules (or kilowatt-hours) required to produce it.

B_j (Joules to produce a block) = N (miners) x H' (avg hash exhaust rate in J/TH per miner) x G hashes (TH) required to produce a block. This J/TH efficiency is also what determines the mining profitability for any given mining rig, as shown in the cost to mine 1 BTC visualization below for an Antminer S9.

Cost to Mine 1 Bitcoin

■ Cost to Mine 1 BTC   ■ Profit   ■ Loss

[Bitmain] Antminer S9

Hardware Efficiency	Break-Even Electricity Price	Margin
88.2 W/Th	0.17 USD	45142 USD
Cost of Production	BTC Mined per Day	Profit per Day
19095 USD	9427 SAT	4.26 USD

Cost to Mine 1 BTC tool on insights.braiins.com

Evidently, utilities get paid in dollars, so you multiply B_j by E (the electricity rate in $/kWh) to get the cost to produce a block $B_\$$. Since the miners won't produce blocks for free, they need to recoup a profit by a combination of the block reward (R), plus the user fees paid (F). That is, $B_\$ < R + F$.

After examining at this basic level, we see that the miners who offer proof of work on behalf of the network are merely engaging in the service of selling block space to the users. It just happens that block price is denominated in electricity, because this is what computers use. "Revolutionary stuff," you may be thinking.
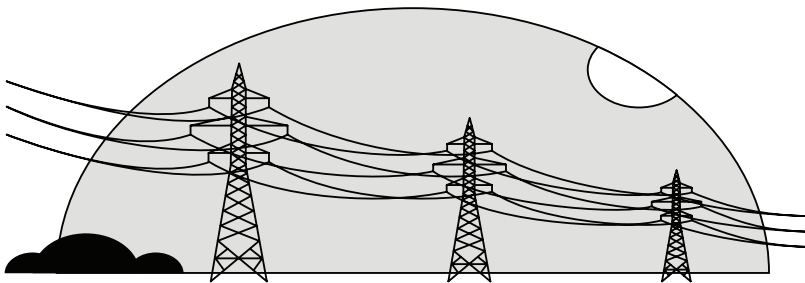
21

$$B_j = N \, x \, H' \, x \, G$$

$$B\$ = B_j \, x \, E$$

$$B\$ < R+F$$

$$B_j * E < R+F$$

Takeaway: the energy expended will always be determined by the rewards available to the miners of the network, including fees for block space.

THE MORALITY OF BITCOIN'S ENERGY USE

Transmission lines

Is it wrong that the electricity consumed by the bitcoin network is significant? Frankly, no. As we showed in the previous section, the electricity used is directly related to the value that users place on its block space. As the demand for block space increases, so do the rewards for miners. This will cause its energy usage to increase as we saw during bitcoin's bull run in 2020.

Clearly, there is demand for the monetary good that is bitcoin, and the block space on which it resides.

Rather than flinging indictments against bitcoin for its energy use—again, a proxy for the value moving across the network—it

would be far more productive to question the sources of energy that produced the electricity that is consumed. Bitcoin uses electricity, and it is agnostic to the fuel source; whether it is carbon-intensive coal, or cleaner sources such as methane waste gas, hydro power, or renewables.

PROOF OF STAKE: A BETTER ALTERNATIVE?

To explain briefly, proof of stake uses tokens that are locked up with a miner ("validator"). Instead of expending compute and energy resources for the right to produce a block, the validator is at risk of destruction of their stake ("slashing") to prevent violations of the consensus protocol.

This would appear to be more efficient, since energy is not directly consumed in the activity of mining blocks. However, the staked tokens are ultimately traded for currency, which in itself is just the distillation of other economic activity. **There is no guarantee that the provenance of the staked capital is any more clean than the energy that is expended in a proof of work mining network.**

Additionally, the capital required to secure a proof of stake network is significantly higher than capital committed to PoW mining equipment (billions versus millions). However, a definite advantage for PoS is that, due to its low direct energy footprint, and concomitant reduced physical size, a proof of stake network may draw less negative attention. At the current time, PoS also has fewer perceived environmental externalities. It is more discrete, for sure.

One final consideration on PoS is that voting power in consensus is determined by the size of stake that a validator has. **Due to the behavior of compounding, larger stakes will increase more quickly than smaller ones, which is a naturally centralizing force on the protocol.** Left unchecked, a dominant stake will pose a risk to censorship resistance, which is already evident in the Ethereum 2 Beacon Chain,

where the top 5 validators comprise over one third of the entire stake—enough to halt or impair the network.

CONCLUSION

Proof of work is a brilliant invention by Adam Back, and an essential component to the bitcoin network. It has roots in defeating Sybil attacks and denial of service, and is what makes bitcoin economically unattractive to attack. Proof of work in bitcoin establishes a pay-to-use communications network, and assigns a cost to block space (bandwidth) that is directly related to the value that its users place on the ability to transact, via fees. Bitcoin miners provide a service, which they consume electricity to provide.

Proof of stake is an alternative method of establishing consensus in blockchains, but the outsized capital required to secure the network may be derived from ecologically costly means, and it has inherent centralizing forces that pose risks to the protocol over time. **For bitcoin, proof of work has proven to be an ingenious solution that is both durable and reliable, despite frequent social, political, and even economic attacks.**

24

Bitcoin Nodes vs. Miners: Demystified

An explanation on the different roles nodes and miners play to support the Bitcoin network. We explore their purpose, requirements, incentives and how each is critical in keeping Bitcoin secure and decentralized.
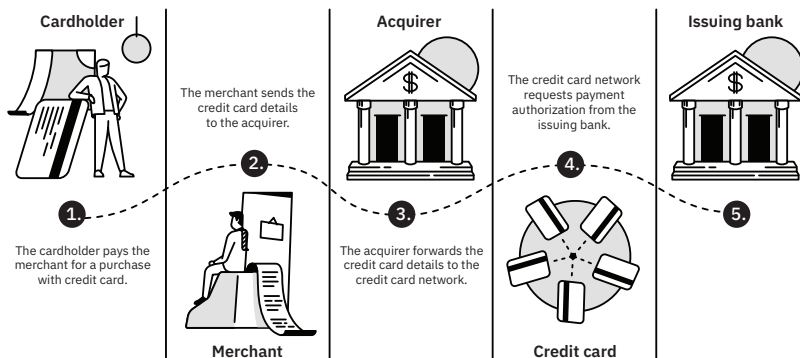
Bitcoin is a complex system that can be hard to fully grasp. This has led many people over the years to dismiss it as just a fad or even a ponzi scheme, rather than recognizing the ingenuity of its design or the greater societal benefits of its continued development and adoption.

One of the simplest ways to understand all the roles and responsibilities of Bitcoin network participants is to follow a transaction from start to finish. By doing so, one can better see the key differences between Bitcoin nodes and miners.

SETTLEMENT: TRANSACTING WITH BITCOIN VS. FIAT CASH OR CREDIT

In the traditional finance world, users send funds from their bank account to merchants for a good or service. This process is generally conducted with a card, app, check, or cash. In the cash example, there is immediate clearing and settlement; once cash is given to the merchant, the transaction is final and irreversible. However, it's no secret that cash is becoming more and more rare as credit cards and mobile payments are gaining popularity worldwide.

With modern payment methods (such as credit cards), there is a lot going on behind the scenes to ensure final settlement. These transactions are facilitated using a few centralized third parties such as banks or payment processors to check that the user has adequate funds available and there is no fraud taking place. These complexities are hidden from the user to ensure a quick and easy experience.
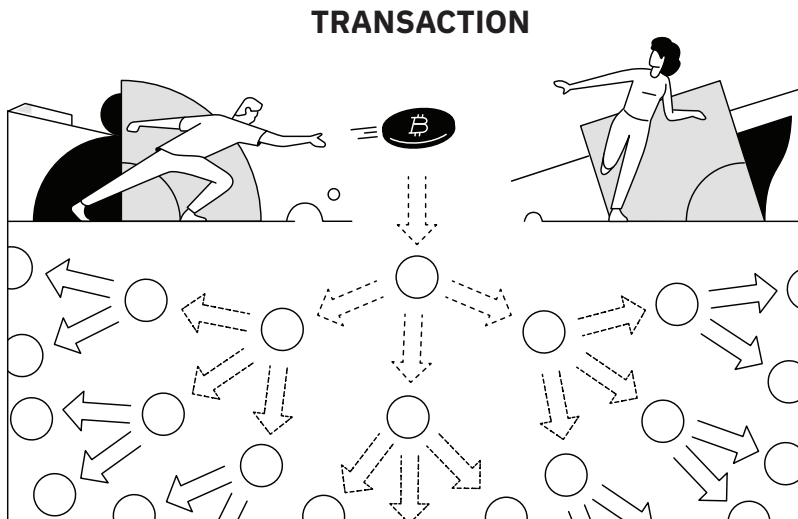
25

Typical digital fiat transaction

The Bitcoin network works in a similar way, where the complexities of facilitating bitcoin transactions are somewhat hidden from the typical user. However, in this system, it's the distributed network of bitcoin node operators and miners that are facilitating the checks on behalf of the user rather than centralized 3rd parties. Miners and nodes form the backbone of the Bitcoin network. Collectively, they are incentivized to facilitate transactions, enforce the network rules, and distribute the 21 million bitcoins. A major difference between these traditional financial systems and bitcoin is that anybody can become a node operator or miner without permission from anybody else. This enables the Bitcoin network to be truly decentralized and difficult, if not impossible to shutdown. To understand more about what miners and nodes actually do, we will walk through a standard bitcoin transaction.

HOW MINERS AND NODES HANDLE BITCOIN TRANSACTIONS

As a user of the Bitcoin network, you primarily want to transact by sending and receiving bitcoin. When a user sends a transaction, it is propagated through the network via gossip protocol. Basically, the transaction is passed to a few nodes who check that it is valid before

26

passing it to more nodes, continuing until all nodes connected to the network are aware of the pending transaction.

TRANSACTION

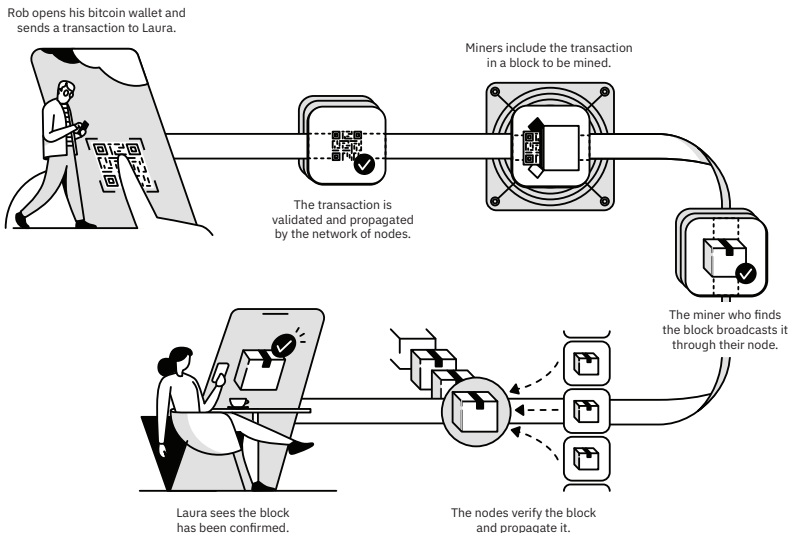Bitcoin transaction propagating through nodes

Nodes hold a full copy of the Bitcoin blockchain, which is a universal ledger system. It contains the complete transaction history of all previous bitcoin transactions. By referencing the blockchain, nodes ensure that the sender of a transaction is not spending the same BTC twice and didn't create it out of thin air.

Once nodes validate a transaction, it's shown in a "pending" state until a specialized node, known as a miner, or a collective of miners (mining pool), picks up the transaction. Bitcoin miners are located all over the world and compete to confirm the pending transactions. Going from a "pending" to "confirmed" state means that the transaction has been added to the universal ledger system (blockchain) and enables the recipient of the bitcoin transaction to send it to another user. The process of mining transactions falls outside the scope of this

article, but is very simply explained in our previous article, "Bitcoin Mining is NOT Solving Complex Math Problems [Beginner's Guide]".

Instead of confirming transactions one by one, miners will batch pending transactions into what are known as blocks. The confirmed block is propagated across the entire network back to all nodes to ensure the block is valid and adheres to the rules of the network. Once validated, the nodes add the block to the previous blocks, thus creating a blockchain.

At this point, the entire network has witnessed this transaction being sent by the user, validated by each node, and confirmed by the miner. Final settlement is achieved and funds are irreversibly passed from the sender to the receiver. This process, relying on thousands of volunteer nodes and competing miners distributed across the world, is repeated for each and every transaction.

Rob opens his bitcoin wallet and sends a transaction to Laura.

Miners include the transaction in a block to be mined.

The transaction is validated and propagated by the network of nodes.

The miner who finds the block broadcasts it through their node.

Laura sees the block has been confirmed.

The nodes verify the block and propagate it.

Lifecycle of a bitcoin transaction

Running through this simple transaction example, you can start to see how nodes and miners differ from each other. They both play crucial roles to the network, and have their own checks and balances to ensure decentralization. Now let's dive a little deeper into the roles of each.

WHAT DO BITCOIN MINERS DO?

Miners, simply put, have 3 roles.

1. Confirm transactions
2. Secure the blockchain
3. Participate in the fair distribution of new bitcoins

Mining bitcoin is a costly endeavor, requiring specialized hardware and using significant amounts of electricity. On top of those economic factors, bitcoin mining also requires significant expertise and entails a lot of risk (unlike operating a node). For example, miners can lose millions of dollars overnight due to extreme weather, floods, fires, and more. To incentivize people to spend resources and take on long-term risk, the Bitcoin network provides miners with the opportunity to earn revenue. Every transaction includes a transaction fee and every block contains a subsidy of newly issued bitcoins, both of which are paid to whichever miner adds the given block of transactions to the blockchain.

Because miners must compete and spend resources to earn newly issued coins, bitcoin is more similar to gold and other commodities than to fiat currencies with unlimited supplies. This unavoidable cost to mine bitcoin is a critical part of its value proposition, as it makes for a relatively fair distribution of newly issued coins and it results in bitcoin being extremely difficult to attack. Nodes play an important role in this as well (as we will describe in the next section).

Currently, about 18.6 million bitcoin have already been distributed to miners through the block subsidy, and this will continue until all

29

21 million bitcoins are distributed around the year 2140. At that point, miners will solely earn transaction fees for confirming transactions and securing the network. However, miners are not all-powerful, but rather they are more like paid servants of the network. **Ultimately, miners must play by the rules enforced by nodes in order to be rewarded with bitcoins.** Nodes, on the other hand, are the true rulers of the network.

HOW BITCOIN NODES KEEP MINERS IN CHECK

Unlike mining, running a bitcoin node is not very costly (it's typically in the $150-$400 range). However, nodes are equally if not more important than miners in achieving decentralization. The roles of nodes are to:

1. Validate transactions
2. Keep a historic record of transactions
3. Dictate and enforce the rules of the network.

In simple terms, nodes ensure that everybody — from miners to users and other nodes — plays by the rules. This can be done out of self-interest. Each user, wallet, company, mining pool, and exchange that runs a node is doing so in part to ensure they are not being cheated. Everyone running a node carries a copy of the blockchain and is responsible for maintaining and updating their copy.

As transactions are propagated and confirmed, node operators are validating that these transactions meet the rules of the network. If a user receives a transaction that creates 1,000,000 bitcoin out of thin air, the user (and all other nodes on the network) will reject the transaction. If any invalid transaction somehow makes it into a block, all the nodes will reject the entire block and wait for another to be mined which doesn't contain any invalid transactions. Bitcoin is based on consensus. All nodes are in agreement to the rules of the network and the state of the blockchain, and will ignore anybody who is misaligned.

30

While there is no direct revenue to be earned by running a node, it is important to run one to ensure you're interacting with the network safely and securely. A node can be installed on any computer with enough storage capacity. A popular approach is to buy $150-$200 worth of components and run a dedicated node on a raspberry pi.

In doing so you can truly be your own bank by running and auditing the Bitcoin network.

YOU DON'T NEED ANYBODY'S PERMISSION

As you've learned, there are similarities between traditional fiat transactions and bitcoin transactions. Both share a complex underlying settlement system that is hidden from the average user.

However, a major difference is the open participation and transparency of said settlement system. Anyone can become a bitcoin node operator or miner without needing permission from anybody else. This completely changes the way commerce can be conducted globally because it eliminates the need to trust or cede control of funds to 3rd party intermediaries.

No one miner or node can control the network. They each put checks and balances on each other to ensure no one cheats the system. A monetary network that is open and permissionless for anyone and everyone to participate can be the backbone of the most resilient, accessible, and inclusive financial system in the world.

This is the power of open networks. This is why millions of people around the world have already voluntarily joined the network.

Whether you choose to run your own full node or become a miner, you're taking part in the open and inclusive Bitcoin revolution. A revolution getting stronger and more unstoppable with each new participant in it.

How Much Would it Cost to 51% Attack Bitcoin?

A thorough explanation of 51% attacks, the possible ways to attempt them, and how feasible each method is today.
Bonus: how we can mitigate the risk with Stratum V2.

When it comes to mining centralization, the big concern that people have is a "51% attack" — where a single actor or group controls a majority of Bitcoin's mining power and can effectively decide which transactions (if any) get confirmed in the blockchain.

Besides just disrupting or censoring the confirmation of new transactions, a 51% attack can also be used for a *double spend.* This means that the attacker mines a different version of the blockchain in secret so that they can spend some coins on the public chain and then later mute the transaction by publishing their version of the blockchain in which they retain ownership of the coins. Another name for this is a blockchain reorganization because it replaces the most recent blocks in the chain.

So far, there have been no successful 51% attacks on Bitcoin in its history, but we have seen successful attacks on other coins like Ethereum Classic. **If successful, such an attack would likely cause significant harm to Bitcoin's reputation.**

MEASURING 1-HOUR COST OF A 51% ATTACK

There's a cool website called Crypto51 which measures the cost to 51% attack Bitcoin and other major proof of work cryptocurrencies. If you go to the About page, it describes how the *1h Attack Cost* is calculated using the current market price (aka *spot price*) for hashrate from NiceHash (NH), a hashrate exchange that allows people to buy

hashpower from miners and control what it's used for. For non-miners, the significance of this may not be clear, so let's explain it.

Supposing that a certain blockchain has a total network hashrate of 100 TH/s, then the cost of a 1-hour 51% attack is the cost of controlling more than 50 TH/s of the hashrate. **If a majority of the hashrate is available on a hashrate exchange, then the 1-hour attack cost is simply the cost of purchasing that hashrate from the market for 1 hour.**

On Crypto51, the portion of a given cryptocurrency's hashrate that's available for purchase is represented by the *NiceHash-able* metric on the right side of the image above. A NH-able value below 100% means that less than 51% of the coin's hashrate can be bought.

For Bitcoin, the NH-able value is under 1%, and other hashrate exchanges do not add much to the value. In other words, the 1h Attack Cost is calculated based on the *spot price* for SHA-256 hashrate, but the volume of SHA-256 hashrate available on the market is not nearly large enough to make it a viable way to actually attack Bitcoin.

Since the value on Crypto51 isn't realistic for Bitcoin, let's dive into more detail about the **different methods that could be used to 51% attack Bitcoin, how feasible they are, and what can be done to mitigate them**. By the end, you'll better understand the security provided by Bitcoin's proof of work system.

BITCOIN CLOUD MINING AND HASHRATE EXCHANGES

For most people, it will never be profitable to mine Bitcoin. This is because competitive electricity prices are typically only found in locations with energy production (e.g., hydroelectric dams, natural gas wells, etc.), not on an urban energy grid.

However, for people who want to speculate on mining profitability, cloud mining offers a way to do so. Cloud mining contracts enable people to "mine" cryptocurrencies without owning the physical hardware themselves. In other words, buyers purchase a specific amount of hashrate for a specific time period and price, then earn the mining rewards produced by that hashrate. Meanwhile, the miners still operate the mining equipment, but they get paid via the cloud mining contracts or hashrate market rather than the mining rewards.

In order to make a clear distinction, from now on we will refer to hashrate sold on an exchange or via cloud mining contracts as **synthetic hashrate**, and hashrate used to mine directly as **physical hashrate.**

So, what does this have to do with Bitcoin's security?

Well, if a malicious actor wanted to attack a cryptocurrency network, it would be far simpler to purchase synthetic hashrate than to produce physical hashrate. However, there's not nearly enough hashpower on hashrate exchanges to consider them as an attack vector against Bitcoin.

That being the case, let's talk about the other possible attack methods.

THE COST OF A 51% ATTACK WITH PHYSICAL HASHRATE

With hashrate exchanges not being viable for accessing 51% of network hashrate, there are only two realistic attack vectors left:

- Amassing enough ASICs (mining hardware) and power capacity to attack the network with physical hashrate
- Controlling mining pools who have a combined majority of the synthetic hashrate

34

Let's start by analyzing the first case. ***How much would it cost to 51% attack Bitcoin with physical hashrate?***

With the current total network hashrate of 150 EH/s, we'll calculate a rough estimate of the costs necessary to set up 150 EH/s worth of ASICs (assuming the miners with the existing 150 EH/s remain honest and don't contribute to the attack). In the most favorable case where all hashrate is produced by an equivalent machine to the highest efficiency ASIC on the market today, the Antminer S19 Pro, then the specifications per ASIC would be 110 TH/s and 3250 W consumption.

150,000,000 TH/s / 110 TH/s = approximately **1.364M ASICs needed to amass 150 EH/s.**

With a per-unit consumption of 3250 W, that would put the **electricity capacity needed to power all those ASICs at ~4.4 GW of power**. That limits the possible candidates to pull off such a huge endeavor to powerful nation states who would work in coordination with large energy producers.

And how much would those 1.364M ASICs cost the taxpayers of such a nation state? Well, at a conservative unit price of $4000 each including power supply units, the **cost of hardware would exceed $5.46 billion.** Factoring in all the R&D costs to catch up to existing hardware manufacturers (who are already sold out until May 2021), plus all the other data center equipment needed, the true cost would likely be far higher.

In the grand scheme, this may still be a small sum to the likes of the USA or China. However, it doesn't account for significant obstacles such as the limited capacity of chip manufacturers like Samsung and TSMC to actually produce these high quality hashing chips. (Not to mention the lunacy of a government using that semiconductor manufacturing capacity to build ASICs and attack Bitcoin rather than any number of other valuable applications.)

Ultimately, attempting to destroy trust in Bitcoin through a mining attack with physical hashrate just doesn't make sense anymore, and it hasn't for years. Nation states who view Bitcoin as a threat are far more likely to over-regulate or (try to) ban its use than to spend billions of taxpayer dollars on mining hardware and power.
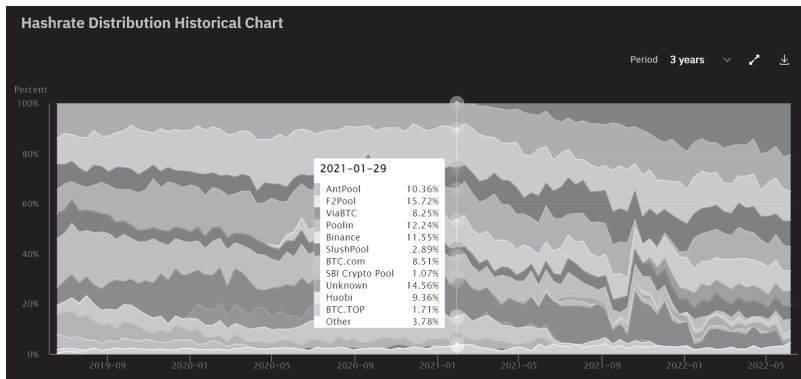
Still, that doesn't mean that 51% attacks are completely impossible. Let's now turn our attention back to synthetic hashrate. This time, instead of talking about hashrate exchanges and cloud mining, we'll discuss mining pools.

SYNTHETIC HASHRATE AND CHINA MINING CENTRALIZATION

Bitcoin mining pool centralization has been a near-constant source of FUD (fear, uncertainty, and doubt) for years. However, it's usually misrepresented. **Mining pool operators have long-term stakes in the Bitcoin network and just as little incentive to attempt an attack as miners themselves.**
You can read an explanation of why hashrate concentration is not a huge cause for concern by searching for a Coindesk article from February 2020 titled, „No, Concentration Among Miners Isn't Going to Break Bitcoin."

A more interesting case to think about is if the Chinese Communist Party (CCP) were to try taking over several mining pool operations. At the time of writing (January 2021), ~97% of Bitcoin's total network hashrate goes through Chinese pools.

36

Pools and Blocks page on insights.braiins.com

It's extremely unlikely that the CCP will attempt any attack. Nonetheless, we'll consider the possibility for a simple reason: attacking with physical hashrate would cost at least $5 billion, whereas attacking with synthetic hashrate by taking over several pools would be essentially FREE.

However, there's a problem with this attack too: **miners can switch pools in a matter of seconds.** If the CCP were to attempt taking over the 4+ largest pools, they would have to hope that no miners switch to other pools so that they can sustain the attack for more than a few pointless minutes.

The less concentrated hashrate is in a few mining pools, the more difficult it would be to attempt a pool attack. However, mining pools are necessary for most miners today to stabilize their revenue, and concentration in a few pools is unavoidable.
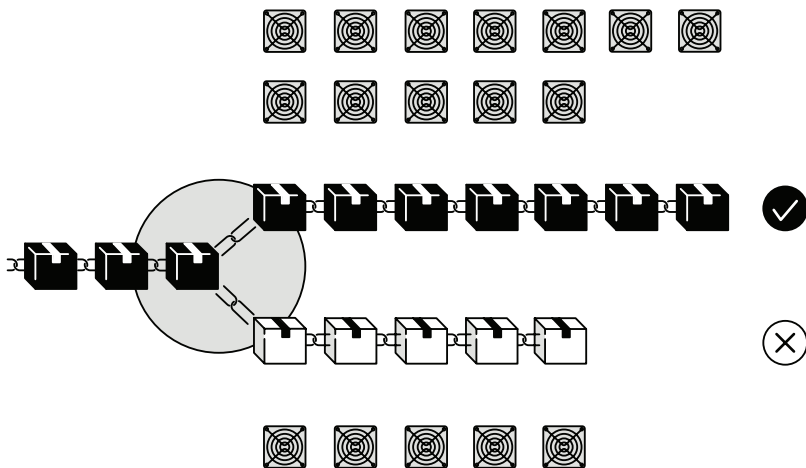
Therefore, one good way to increase the difficulty of a mining pool attack is to make it impossible to do covertly.

In other words, the attack causes more damage the longer it is sustained, so it can be mitigated by ensuring that some miners would detect it within minutes and switch pools.

BLOCKCHAIN REORGANIZATIONS

Every block in the blockchain references the block before it with a value in the block header called the *prevhash*. With Stratum V2, miners will be able to construct blocks themselves with data from their own nodes (a process called *Job Negotiation*), so if they are honest they'll always reference the prevhash of the most recent block in the chain.

By taking block construction out of the pools' hands, Stratum V2 can help miners ensure that they won't contribute to secretly mining a "shadow" chain that gets broadcasted later in a blockchain reorganization attack. Similarly, they can ensure that their hashrate is not used to mine a different SHA-256 chain, such as Bitcoin Cash or Bitcoin SV.

The chain with more work wins

The chain with the largest block height is considered valid, so mining a longer chain in secret and then broadcasting it later can overwrite all the blocks that were mined publicly in the meantime. **If a pool rejects valid block templates proposed by their miners, those miners could automatically switch to another pool.** That is the potential benefit of Stratum V2 Job Negotiation from a decentralization standpoint.

THE COST TO 51% ATTACK BITCOIN DEPENDS ON THE TYPE OF ATTACK

To summarize everything above, there are essentially two ways to attempt a 51% attack:

- **Physical hashrate**: purchase or manufacture ASICs and run them, costing ~$5.5 billion as a conservative estimate at the time of writing. Alternatively, simultaneously take control of enough individual mining farms to pull off the attack, an extremely difficult coordination problem likely involving 100+ operations.

- **Synthetic hashrate**: simultaneously take over 3-5 mining pool operations and mine empty blocks or do a deep reorg attack in an attempt to break user trust in Bitcoin. Still difficult to coordinate, but essentially free if the attacker doesn't have a long-term stake in Bitcoin.

Since the synthetic hashrate attack vector is practically free while the physical hashrate attack vector is far more complex and costly, it makes sense to focus on increasing the difficulty of attacking with synthetic hashrate. Stratum V2 can do just that.

GO READ MORE:

How to Mine Bitcoin [Beginner's Guide]
A guide to help you decide if you should start mining
Bitcoin and what to doin order to get started.

What Happens When Two Blocks are Mined
Simultaneously? Bitcoin Chain Splits Explained
Understanding why temporary chain splits (i.e. forks)
naturally occur, how the bitcoin protocol handles
them in a decentralized way and what happens to
your coins during temporary forks.

A Summary of Bitcoin's Energy Consumption
Debate
An overview of the information that usually gets
left out when Bitcoin mining's environmental
impact becomes a mainstream talking point.

MINING SOFTWARE

There's a famous quote from Plato that goes "necessity is the mother of invention." Looking at the evolution of the bitcoin mining industry and our contributions to it, this certainly rings true. From professionalizing and enhancing the pool with new features over the years, to launching Braiins OS for Antminer S9's in 2018 and the first firmware + pool implementation of Stratum V2 in 2020, most of our software contributions to the bitcoin mining industry have been driven by necessity for more scalable services for miners and to counteract centralizing forces.

In 2018, Bitmain had at least 80% market share for ASIC manufacturing and was publicly outspoken in support of SegWit2x and later Bitcoin Cash, with just months passing since discoveries of covert AsicBoost and the Antbleed backdoor in the S9 firmware. This pushed us to release Braiins OS with overt AsicBoost enabled and fully auditable, open-source code in 2018. Then, as AsicBoost became the default and competition in mining got fierce with the 2020 halving approaching, we jumped into the autotuning game with Braiins OS+, which now runs on hundreds of thousands of machines globally. Miners running Braiins OS+ and connected to Slush Pool are also the first in the industry to benefit from more efficient and secure (encrypted) data transfers with Stratum V2.

With many of our projects, the first obstacle in adoption has been a lack of understanding. How do mining pools work? What is autotuning? Why should we use Stratum V2? And so on. In this section, we shill both our commercial and open-source projects through detailed explanations of how the software works and what advantages it offers.

Autotuning vs. Overclocking for Bitcoin Miners (SHA-256 ASICs)

Describing the two main methods Bitcoin miners use to increase their revenue and how they can be most effective when used together.

Let's skip the usual slow introduction and get right to the topic at hand: how Bitcoin miners can increase revenue. Generally speaking, there are 2 ways for a Bitcoin mining operation to boost their top line:

- Buy new hardware
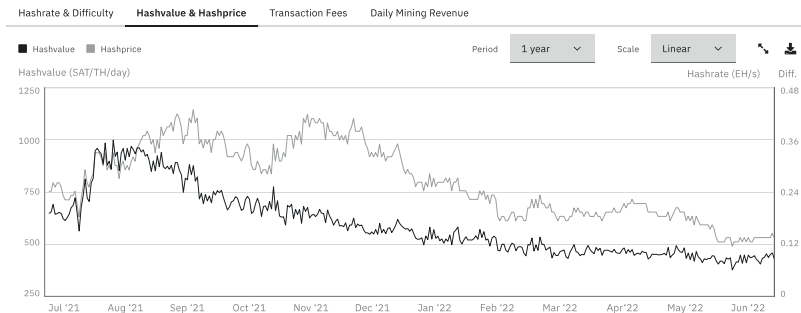- Improve the performance of their current hardware

Buying new hardware is the riskier option of the two, as it typically involves a large up-front capital expenditure that will likely take many months or even years to get a positive ROI, subject to Bitcoin's price performance of course.

In comparison, getting more from existing hardware is a no-brainer for most miners. What's less obvious or well-known is that **overclocking is not the only way to increase an ASIC's hashrate**. In this article, we'll explain how autotuning firmware can boost miner revenue and how it's different from the better-known practice of overclocking.

OVERCLOCKING = MORE HASHRATE, LESS EFFICIENCY (MAX W/TH)

Sometime around early 2018, miners began experimenting with overclocking their ASICs to boost revenue. Overclocking simply means that the ASICs consume more power, hash at higher frequencies, and produce more valid proofs of work than at stock settings. For example, an Antminer S9 that typically produces 13.5 TH/s at 1200 W consumption

42

could be overclocked to produce 16 TH/s at 1600 W consumption instead. With Bitcoin difficulty adjusting upwards consistently as more and more ASICs come online, the revenue produced by a single machine typically decreases substantially over time.

Mining Economics charts on insights.braiins.com

The hash price ($/TH of hashrate) has consistently dropped over time as difficulty has risen.

Therefore, miners want to get as much out of their machines as possible, as quickly as possible, before their profit margins get squeezed thin by the rising difficulty. And they are willing to make their machines less efficient (i.e. higher W/TH) with overclocking in order to stack more sats in the short term.

However, the potential firmware improvements do not stop at overclocking.

AUTOTUNING = MORE HASHRATE, MORE EFFICIENCY (MAX TH/W)

Something many people don't realize about ASICs is that every individual device is unique in terms of the quality of the hashing chips and the overall manufacturing. This is primarily due to the fact

43

that silicon quality is not 100% uniform, so some hashing chips are naturally better performing than others.

However, mining companies require standardization when they are purchasing hardware, so manufacturers typically make the ASIC specifications much lower than the maximum performance possible in order to better ensure that every machine they deliver will meet miners' expectations.

On that note, a lesser-known performance upgrade for ASICs that's similar to overclocking is known as autotuning. Both overclocking and autotuning involve adjusting the frequencies on the hash boards in order to alter the ASIC's performance. The difference between overclocking and autotuning is in the intelligence and sophistication of those frequency adjustments.

You see, overclocking is a rather brutish adjustment. Simply increase the frequency on the hash boards in order to increase the machine's hash rate. Autotuning, on the other hand, is far more sophisticated. Rather than increasing the frequencies of entire hash boards, **autotuning firmware can calibrate the frequency on a per-chip basis.** In other words, the firmware finds an optimal frequency for every individual chip, sending higher frequencies to higher quality chips or lower frequencies to lower quality chips.

The end result from autotuning is a better W/TH efficiency at any power setting the miner chooses. **When combined with overclocking, autotuning can enable even higher hashrates or it can maintain the same hashrate increase while bringing power consumption down.**
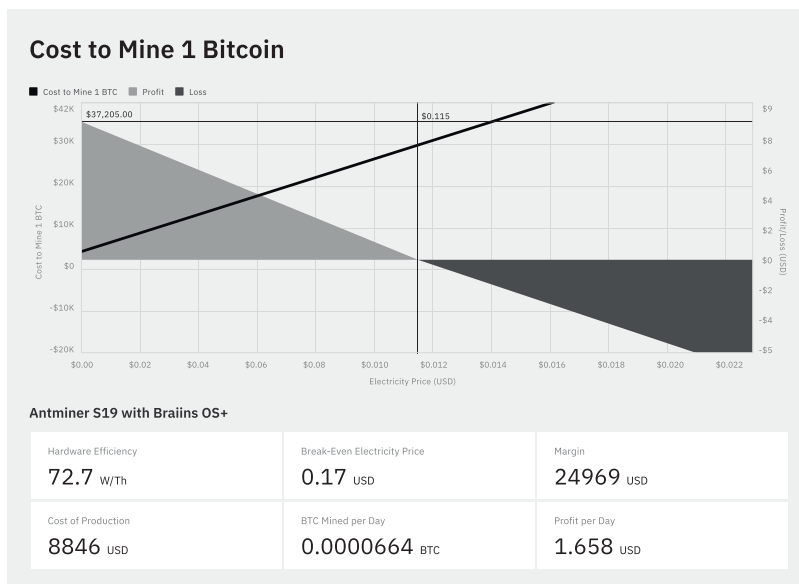
For example, the same Antminer S9 that typically produces 13.5 TH/s at 1150 W consumption with stock firmware could produce 15.5 TH/s at 1150 W consumption with a per-chip autotuning firmware.

44

For miners who have very cheap or even free electricity, overclocking + autotuning is the most effective way to maximize the amount of BTC mined.

USERS CHOOSE THE POWER LIMIT

In bull markets, autotuning and overclocking tends to be the most common combination as miners aim to maximize revenue while they have better profit margins. However, autotuning optimizations are useful across a full spectrum of mining strategies.

For example, autotuning at low power limits was very useful for miners using Antminer S9s around the time of the last halving when profit margins were squeezed thin. With Braiins OS+, miners can set their power limit at 800 or 900 Watts for S9s and achieve an efficiency in the 70-75 W/TH with air cooled machines, as shown with our cost to mine 1 BTC calculator. (Miners can achieve ever better results with immersion cooling.)

Cost to Mine 1 Bitcoin

Antminer S19 with Braiins OS+

Hardware Efficiency	Break-Even Electricity Price	Margin
72.7 W/Th	0.17 USD	24969 USD
Cost of Production	BTC Mined per Day	Profit per Day
8846 USD	0.0000664 BTC	1.658 USD

Cost to Mine 1 BTC tool on Braiins Insights

The key value proposition of autotuning firmware is that it will optimize ASIC efficiency at any power limit that you specify, lowering your costs for every satoshi of revenue you earn.

THE MARKET FOR AUTOTUNING FIRMWARES

Everybody who's been in mining for a few years understands how quickly the mining industry evolves. **While autotuning is still relatively uncommon today, it will likely become a standard practice among miners within 1-2 years**. Miners have several 3rd party firmware providers to choose from, which is a huge improvement from just a few years ago when Bitmain was the dominant hardware manufacturer and there were no custom firmwares for Antminers.

In recognizing the value that autotuning can provide — particularly to miners outside of China who have to wait longer and pay higher prices for new-generation mining hardware — we at Braiins have dedicated ourselves to developing a high performance autotuning firmware for mining operations of all sizes.

Braiins OS+ is competitive with other ASIC optimization firmwares on cost and performance, but unique in other key aspects such as the open-source foundation, GPL compliance, and the solid reputation that we've built through over 7 years of experience in Bitcoin mining.

Bitcoin Mining Pools: Luck, Shares, and Estimated Hashrate Explained

How pool luck is calculated, what shares are and why they are so important in pooled mining, plus the difference between estimating pool hashrate based on blocks found versus measuring pool luck.

"We haven't found a block in X hours, is something wrong with the pool?"
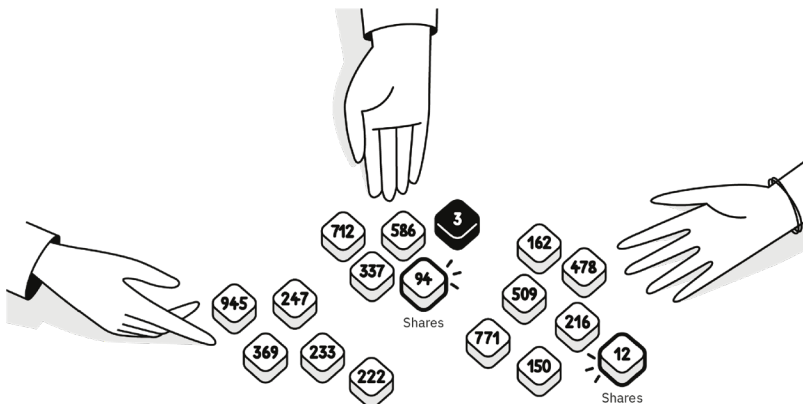
Short answer: no.

Long answer: the mining rabbit hole is deep, let's dive in.

BITCOIN MINING POOLS ARE LIKE MINI VERSIONS OF THE BITCOIN NETWORK

One of the things you learn as a beginner to bitcoin mining is the purpose of network difficulty and the difficulty adjustment. In case you aren't yet familiar with these, you can read our simple explainer, Bitcoin Mining is NOT Solving Complex Math Problems, which we will build on below.

To understand how mining pools work, fortunately you just need to apply the same concept of network difficulty, but at a smaller scale. You see, in order to find a block, miners must compute a hash which has an output below the network difficulty target. This doesn't happen very often—on average, once every 10 minutes.

47

Difference between shares and block finds

Network difficulty example: only dice rolls below "4" (network difficulty) can produce new blocks.

In the article linked above, we used an analogy comparing hashing in bitcoin mining to rolling many-sided dice. The network difficulty target says how low the dice roll needs to be to produce a block.

Similarly, in order to earn a reward from a bitcoin mining pool, you have to compute a hash which has an output below what's known as the "share difficulty target". This is a middleground... much easier to meet than the network difficulty target, but still difficult enough that only a tiny portion of all the hashes you're computing will qualify.

Re-using the same dice analogy, this share difficulty could be incorporated by saying that all the dice rolls below "99" result in shares being submitted to the pool, while they still have to be below "4" to produce a new block.

Share difficulty example: Dice rolls below "99" (share difficulty) can produce shares, while they still have to be below "4" to produce blocks.

48

Sumary:

- Hash outputs < 4: produce a block (and shares)

- Hash outputs < 99: produce shares

- Hash outputs > 99: doesn't meet target, nothing sent to the pool

Anytime your ASICs produce shares, they are sent to the pool to earn mining rewards. To verify the validity of the shares you submitted, the pool simply repeats the same hash computation that you did to produce the shares in the first place. Getting the same result verifies that the proof of work is valid. (Note: "stale" or "rejected" shares can occur when you submit shares after the block for those shares has already been found, something which typically occurs in the few milliseconds immediately following a block find. This is why it's advisable to connect to the nearest pool stratum server to your geographic location.) From this description, can you see why shares are so important? **To verify the shares, the pool must compute the hash... meaning that, without shares, pools would have to redo ALL the hashes that miners do just to be sure that miners are actually doing the work in the first place.** In other words, public mining pools couldn't exist without shares, as they wouldn't have an efficient way of measuring the hashrate of each miner connected to the pool in order to fairly distribute the rewards.

This also explains why your pool hashrate fluctuates somewhat even when you have perfect uptime. Sometimes you'll "find" shares faster than expected based on your hashrate and share difficulty target, and sometimes slower. The same way that sometimes miners find 2 blocks in a matter of seconds, and other times no blocks for 30+ minutes. **Variance is a part of mining at every scale**. In this sense, **pools and share difficulty targets are like mini versions of the bitcoin network and its network difficulty target**. The same math applies to both.

49

One thing to note is that there is no single share difficulty target for all the miners in a pool. Since shares only exist to be a practical unit for pools to measure miners' hashrate, the share difficulty target can be adjusted for each individual miner based on their hashrate. For example, a miner with 100 PH/s will have a higher share difficulty (i.e. lower target for the hash output value) than a miner with 15 TH/s. The goal in setting this share target is for miners to be submitting shares about once every 2-3 seconds, providing a good balance between measuring your hashrate accurately and minimizing computational intensity for the pool to verify the work of all its miners.

THE MARKET FOR AUTOTUNING FIRMWARES

Before we move on, something else to understand about shares is that they aren't produced one at a time. Rather, one hash computation which has an output below the share difficulty target produces many shares. The number of shares produced equals the number of proofs of work done multiplied by the share difficulty. To put it simply:

- 1 share = 1 proof of work on difficulty 1

- 5 shares = 1 proof of work on difficulty 5 (or 5 proofs of work on difficulty 1)

- 100 shares = 1 proof of work on difficulty 100 (or... you can see the pattern)

To illustrate further, suppose that we have a large miner with share difficulty 10,000 and a smaller miner with share difficulty 100. Both miners submit one hash (i.e. 1 proof of work) every 2-3 seconds on average, but that 1 hash accounts for 10,000 shares for the larger miner and 100 shares for the smaller one.

This is how the pool is able to validate the work of larger miners without linearly scaling the pool's own work. They still just need to run

a single hash computation, but it represents more shares the higher the difficulty was in producing it.

HOW BITCOIN MINING POOL LUCK IS MEASURED

If you find yourself confused by the concept of "luck" in mining, you're not alone. In Slush Pool's 11+ year history as of 2021, luck has been the most frequent topic of questions. In order to fully grasp how it works, you first have to know about shares, which itself is not common knowledge. But now that you've read about shares, let's get to luck.

Pool luck is defined as the *expected number of shares to find a block divided by the actual number of shares it took for the pool to find a block*. This *expected number of shares* is based on the network difficulty, where higher difficulty means that the expected amount of shares required will also be higher.

For a simple example with made up numbers, suppose that a pool has 10 miners each submitting 10 shares per second on average, for a total of 100 shares per second. Also suppose that the total expected number of shares to find a block with the current network difficulty is 600,000. At a rate of 100 shares / second, it will take 6,000 seconds (100 minutes) to accumulate 600,000 shares. In other words, the pool should find a block once every 1 hour and 40 minutes in this scenario, assuming constant network difficulty and pool hashrate.

Now let's suppose the pool found a block after only 300,000 shares instead of 600,000. The pool luck for that block would be 200%, as it's 600k/300k*100% = 200%. Alternatively, suppose it takes 1,200,000 shares to find a block. Now the luck for that block is 600k/1200k*100% = 50%.

This means that the pool luck cannot adjust until the pool finds a block, as it's unknown how many shares it will take until the block

51

find actually occurs. Luck is a static value that updates occasionally, not a dynamic one updating constantly.

However, you can still get a rough idea for what the luck would be if the block find occurred at the present moment by dividing the *Avg. Round Duration by the actual Round Duration.* The *Avg. Round Duration* is calculated with the expected number of shares to find a block (based on network difficulty) and the expected amount of time to accumulate those shares (based on the pool's hashrate.)

Fluctuations in the pool hashrate impact the rate at which more shares are accumulated, increasing the *Avg. Round Duration* when the pool hashrate drops and vice versa when the pool hashrate goes up.

It's also important to notice what *does NOT* directly impact the *Avg Round Duration*, nor the pool luck: blocks mined by other miners / pools. Mining is probabilistic, and the probabilities don't change based on past history of the pool nor the luck of other miners. **Every hash is just as likely to result in a block find as every other hash**. Likewise, if it's expected that 600,000 shares will be needed for the pool to find a block, it doesn't matter whether other miners / pools find 20 blocks or 0 blocks in that time—**the only things that matter for pool luck is the quantity of shares submitted to the pool and the network difficulty**. And of course, remember that luck always trends towards 100% over time—it's just math.

HOW POOL LUCK TRANSLATES TO MINING REWARDS

Finally, let's move on to the question most of you probably came here to answer. That is, *how does all of this affect my mining rewards on Slush Pool?*

In a simple world where you are maintaining a constant share of the pool's total hashrate, luck translates 1:1 with your actual vs.

expected mining rewards. If the pool luck is 100% in a 10-block period, it means that the pool found exactly as many blocks as expected given the pool's hashrate in that time. If your portion of the pool's hashrate didn't change over that 10-block period, earning 100% of expected rewards applies to you as well. Likewise, 200% luck would mean you earned 2x more than expected, while 50% luck would mean you earned 50% as much as expected.

In the real world, the answer depends. For example, if you have downtime during a period of no blocks and you have full uptime when all the 10 blocks are found, you'd earn more than expected for your hashrate when the pool has 100% luck. On the other hand, downtime during block finds would result in earning less than expected when the pool has 100% luck. However, note that this doesn't apply for more hashrate joining the pool. When the pool's hashrate increases while your individual hashrate stays constant, you will earn a smaller portion of rewards for each block. At the same time, though, the increase in the pool's total hashrate results in reaching the expected amount of shares to find a block more quickly. **Put another way, it means the pool should find blocks more often, so your reward per block goes down but the frequency of block finds offsets it**.(This is with constant network difficulty.)

Every hash is just as likely as any other to produce a new block, meaning there is no way to try to "time the market" so to speak. You can try to "sell high" by scheduling downtime or hopping pools right after a block find, but the probability of another block find occurring is just as likely as at any other time. You can also try to "buy low" by joining the pool during a bad luck streak, but a long round doesn't make it any likelier for the next hashes to result in a block find, either. In fact, since mining is pure math without any human emotion element (unlike markets), it is even more pointless to try to time it. **Just keep hashing and remember that luck always trends towards 100% over time.**

ESTIMATING POOLS' HASHRATE BASED ON BLOCKS FOUND

Since per-block pool luck is only a function of the blocks mined by the pool, it doesn't change based on the rate at which other miners are finding blocks nor as a function of time—it's based purely on shares. A metric which does incorporate the general passing of time and other blocks being mined is the pool's estimated hashrate.

We estimate the hashrate of every miner / mining pool on our Bitcoin Mining Insights dashboard using the network difficulty and the number of blocks found by each entity during a given period. At the time of writing, the period we use is 720 blocks, which works out to 5 days of mining activity if the average block time is 10 minutes. (Note: this is why different dashboards can have different numbers—there's no one "correct" way to do it.)

Bitcoin Mining Pools Hashrate Distribution

Pool		HQ	Reported ⓘ Hash Rate	Estimated ⓘ Hashrate	Blocks Mined 1D	5D	2W	Avgerage Block Value	Market Share
1	Foundry USA Pool		47.71 EH/s	54.20 EH/s	40	179	1078	6.365 BTC	22.95 %
2	F2Pool		36.13 EH/s	36.13 EH/s	26	115	725	6.369 BTC	15.30 %
3	AntPool		33.20 EH/s	42.39 EH/s	29	141	741	6.368 BTC	17.95 %
4	Binance		24.22 EH/s	22.03 EH/s	21	73	520	6.368 BTC	9.33 %
5	ViaBTC		22.03 EH/s	15.76 EH/s	9	56	507	6.369 BTC	6.67 %
6	Poolin		21.68 EH/s	21.68 EH/s	15	79	537	6.355 BTC	9.18 %
7	SlushPool		13.01 EH/s	13.15 EH/s	11	47	291	6.368 BTC	5.57 %
8	BTC.com		9.838 EH/s	9.838 EH/s	4	33	165	6.351 BTC	4.17 %
9	Luxor		6.08 EH/s	8.861 EH/s	4	28	129	6.375 BTC	3.75 %
10	SBI Crypto Pool		4.41 EH/s	6.233 EH/s	3	19	108	6.360 BTC	2.64 %
11	MARA Pool		3.278 EH/s	3.278 EH/s	1	10	49	6.358 BTC	1.39 %
12	Unknown		1.314 EH/s	1.314 EH/s	1	5	144	6.389 BTC	0.56 %

Pools Rankings on insights.braiins.com as of June 2022

As long as pool operators are honest in reporting their hashrate, the reported hashrate values will always be more accurate than the estimated hashrate values because estimated hashrate incorporates the natural short-term variance in bitcoin mining.

54

Longer time periods should reduce this variance, but using too long of a time period can cause the estimated hashrate value to significantly lag the real hashrate value. 720 network blocks is a period we feel balances these two factors. With reported hashrate being a real-time stat while estimated hashrate is over a longer time period, it's not precise to calculate pool luck with these two values. It can certainly give you a general idea, but any significant changes in the pool's hashrate during the analyzed time period (720 blocks on Mining Insights) will not be reflected properly.

Final thought: no matter how long you're in mining, the difficulty adjustment never ceases to amaze.

Hashrate Robbery: Stratum V2 Fixes This (and More)

Why hashrate hijacking is such a big problem for miners and how it's solved with the improved security of Stratum V2.

Bitcoin's resilience to change is one of its most important features in becoming a trusted store of value. At the same time, however, it makes patience a necessary virtue for Bitcoiners when key upgrades such as Schnorr and Taproot take years and years to implement safely.

When it comes to mining, things are a bit different. Change doesn't happen overnight, but it's also true that miners who don't adapt and keep a finger on the pulse of the industry are likely to get left behind sooner or later.

Consider that Bitcoin's total network hashrate has increased by nearly 200% in the past year alone. Ultimately, that means that everybody in the mining industry is on the lookout for an advantage over their competition. Or, at the very least, a way to keep up.

So, why are we telling you this?

Well, the reality is that mining is probably the least understood area of the Bitcoin ecosystem. After publishing the Stratum V2 documentation and specification, we saw that general Bitcoiners took it completely differently than actual miners.

While the former camp was almost entirely focused on the decentralization improvements from work selection, the miners were focused on everything else. And this is why we want to share some insights from within the mining industry.

You see, work selection is an extremely important part of Stratum V2, and one that can improve Bitcoin's fundamentals in the coming years. But it's not going to drive adoption in the short term. Rather, it's features such as hashrate hijacking prevention and significant efficiency improvements that can incentivize adoption to occur throughout the mining industry.

In this article, we'll explain what those features are in greater depth and why they matter to the people who matter, the miners.

A BITCOIN MINER'S PERSPECTIVE

When Slush Pool mined its first block in 2010, most mining was happening on the personal computers of enthusiasts in North America and Europe. For context, a single new-generation ASIC today has roughly 700x more hashing power than the entire network did back then.

The technology has come a long way. At the same time, the business side of the mining industry has gone from nonexistent to ultra-competitive.

Today's miners are typically focused much more on their bottom line (i.e. net profit) than on Bitcoin's fundamentals. That's not to say that there aren't any ideologically-driven miners out there who care deeply about Bitcoin's success — there are still many. However, the point is that the people running large mining farms with hundreds of petahash can't be expected to switch to Stratum V2 and choose their own work merely because it improves decentralization.

If Stratum V2 doesn't impact a miner's bottom line, it's probable that miners aren't going to switch to it. With that in mind, we know that there are two ways for a business to raise its bottom line:

- Increase revenue
- Decrease costs

57

It's possible that some entrepreneurial miners will think of new business cases that are enabled by Stratum V2, but in the majority of cases, it will be decreasing costs that incentivizes miners and pools to switch. **So let's talk about why even the most business-oriented and least ideologically-driven miners out there would start using Stratum V2 in their operations.**

HASHRATE HIJACKING IS A PROBLEM

Stratum V1 has a major security flaw: it's vulnerable to man-in-the-middle (MITM) attacks. The worst of these attacks is hashrate hijacking, in which a malicious third party is able to steal a miner's proof of work before it reaches their target pool, thereby taking credit for the work and earning the payout for themselves instead.

To make matters worse for miners, an attacker can steal their hashrate completely undetected. If the attacker is smart and stealthy, they might steal only 1% or 2% — enough to impact the miner's bottom line, but not enough for the miner to be sure that they are being attacked rather than underperforming expectations for some other reason.

The good news: Stratum V2 fixes this. **Connections between miners and pools in V2 are encrypted with a scheme known as authenticated encryption with associated data (AEAD), which protects the integrity of the data transfers.**

Currently, we are aware of miners from China, Kazakhstan, Russia, and Europe who strongly suspect that they are having hashrate hijacked. Considering that we only have contact with a small percentage of the miners in the global community, it's possible that this problem is far bigger than anybody realizes. Furthermore, the mere risk of hashrate hijacking is a strong business incentive for operators to switch to Stratum V2 and start encrypting

their communications. **The fact that hashrate hijacking can occur undetected over a long time period makes it a problem worth solving for everybody, regardless of whether they think it's happening to them right now or not.**

EFFICIENCY IMPROVEMENTS BRING DOWN OVERHEAD COSTS

Running a public pool service with a global consumer base is not a cheap task. It requires staffing a qualified development team and maintaining geographically distributed servers in close proximity to as many mining operations as possible.

Every day at Slush Pool, we process millions of data transfers across tens of thousands of individual physical connections. Stratum V2 decreases both the size and quantity of those data transfers. In other words, **it makes running a pool service easier and more affordable too.** That's certainly an incentive motivating us to develop the protocol, and we hope it incentivizes other pools to adopt it as well.

As for the actual miners, efficiency improvements may not be as strong of an incentive for some as for others. Many miners pay flat rates for hosting their machines which include the costs of internet infrastructure and data used to communicate with pools. There are numerous others, however, located in extremely remote places where data is costly and bandwidth speeds are limited. For them, the switch to binary and other efficiency improvements can create a substantial improvement.

Moreover, Stratum V2's multiplexing feature makes it possible for miners to mine multiple coins on a single connection as well as doing zero-time backend switching. In other words, miners can more efficiently implement use cases like coin switching to increase profit

(e.g., Bitcoin, Bitcoin Cash, and Bitcoin SV) or even send hashrate to multiple pools at once on a single connection.

Finally, a simplified mining mode for ASICs called header-only mining gives miners the option to avoid merkle path handling, simplifying firmware and making work validation lighter for pools. Header-only mining makes it easier to manage large operations, streamlines future protocol upgrades, and results in lower hashrate variance for miners.

All of this adds up to three things for end miners:

1. **Less complexity to set up and run a mining operation**

2. **Lower costs for internet infrastructure and better performance in remote locations**

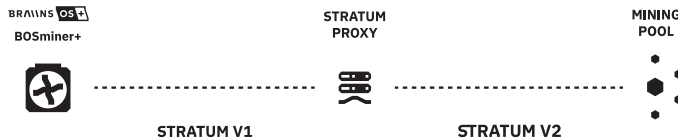3. **Enabling more complex use cases that can increase revenue and /or lower costs**

FULL IMPLEMENTATION IN BOSMINER MAKES SWITCHING TO STRATUM V2 EASY

There's a famous movie line from Field of Dreams, "If you build it, they will come." This is NOT our approach to Stratum V2 adoption.

Designing and publishing the protocol is not enough to achieve meaningful adoption on its own, and we know it. Fortunately, we at Braiins do more than solely operating Slush Pool. We also develop firmware for ASICs. And because of that, we can develop a full implementation of Stratum V2 in our BOSminer software component, which will be free and open-source for the entire Bitcoin mining community.

In addition, we've developed translation proxies for V2 -> V1 and vice versa, meaning that miners can use V2 while mining on a pool that

60

doesn't support it and that pools can implement V2 without forcing
their miners to use it.

Translation proxies for Stratum connections

**This means that miners who want to use V2 in their operations
won't have to jump through tons of hoops and in-house development
to do so. Instead, they'll be able to simply replace CGminer with
BOSminer on their machines and they're ready to go.**

By drastically minimizing the cost to switch to Stratum V2, we believe
that the incentives described in the sections above are enough
to attract a group of early adopters. If the early adopters have
a better experience as a result, the rest of the industry will follow.

THERE'S STILL A LOT OF WORK TO DO

We've been in the mining industry longer than anybody, so we know
its pain points and problems well. Stratum V2 was designed to solve
as many of those issues as possible, and we're confident that it will
make life easier for just about everybody. To recap, V2 adoption will
be driven by:

- Hashrate hijacking prevention

- Efficiency improvements that lower overhead costs

- Ease of switching thanks to full implementations that are
  open-source and available to everybody.

Still, it's important to point out that the specification is not yet finalized,
and Stratum V2 isn't a finished product. So on that note, it's time to
get back to coding.

Bitcoin's Decentralization with Stratum V2

Explaining how Job Negotiation works in Stratum V2 and how it improves decentralization of Bitcoin mining.

With the recent news that Square Crypto is looking to support Stratum V2 development with a grant, we thought it was time that we explain more about how Job Negotiation works and the benefits it provides.

We'll start with a technical explanation of the pooled mining process with both Stratum V1 and V2, as this hasn't been explicitly explained in the documentation on stratumprotocol.org and it's really important if we are to understand the actual improvements V2 makes. Then we'll address two of the most common concerns we've heard from miners about the practicality of enabling miners to choose their own work in Stratum V2. From there, we will walk through one of the biggest theoretical attacks many Bitcoiners worry about, the "state attack." And finally, we'll describe how it all fits into the modern mining industry from a short-term and long-term business perspective.

WHY IT'S CALLED JOB "NEGOTIATION"

First, let's go through the order of operations so that everybody is on the same page.

If you aren't already familiar with how mining pools operate, we recommend you read the relevant sections of Mastering Bitcoin.

Stratum V1

Presently, this is a summary of how work is typically done in pooled mining:

1. Miner connects to pool

2. Pool sends miner job assignments (i.e. block templates to work on, without full transaction sets)

3. Miner does work (i.e. plugs in nonce values looking for hashes below the difficulty target)

4. Miner sends proof of work (i.e. nonces leading to "good enough" hashes) back to pool

5. Pool validates the proof and broadcasts blocks when found

6. Miner gets paid for their submitted proof of work (so called „shares")

Pools and solo miners are the only entities that are constructing block templates. Regular miners cannot because they don't have the transaction sets to build the blocks.

Stratum V2

This is a simplified overview of how pooled mining will work in the future for miners who choose to construct their own blocks:

1. Miner connects to pool

2. Job Negotiator (i.e. software run by the miner or 3rd party between miner and pool) sends request to the upstream pool node to work on a block template

3. Pool verifies that the transactions included are valid*

4. Pool verifies coinbase transaction outputs are correct (i.e.paid to the pool address)

5. Pool accepts the proposed block template**

64

6. Miner works on their own block template

7. If a block is found, the miner can propagate the block themselves and censorship by the pool is not possible

8. Miner gets paid for their submitted shares

Since block propagation does not necessarily depend on the pool node, it occurs as rapidly as it would if the miner were simply solo mining.

*Economics of Job Negotiation

An important question that arises is how payouts will be handled when miners can be working on different blocks while part of the same mining pool. The answer is that **every miner is paid based on the value of the shares they submit, not based on the value of the block that gets mined.**

For instance, suppose there are two block templates being worked on by the miners of a single pool:

- Block Template 1 value: 8.0 BTC

- Block Template 2 value: 7.5 BTC

Miners working on the 8.0 BTC block will be paid proportionally more for their valid shares than those working on the 7.5 BTC block. This means that miners with well-connected full nodes may be able to work on blocks that are more valuable than those distributed by the pools themselves, thereby increasing their payouts relative to the miners who aren't proposing their own block templates. More importantly, it means that miners who propose blocks with lower value transaction sets will receive proportionally lower payouts,
but they won't impact the payouts of the miners in the rest of the pool.

65

**Latency concerns

Another point worth discussing is what happens in the moments immediately after a new block is found and propagated. The Job Negotiation process can take several seconds, and every second counts when searching for nonces. This gray area can be addressed with an asynchronous start, which means that miners can begin working on their own blocks immediately while the pool is still validating them. Once the pool validates a proposed block template, the work already done by the miner(s) is paid for accordingly. In the event that a miner proposed an invalid block template, the shares from those few seconds of work are rejected and don't earn payouts. A proposed block template can be rejected for two reasons:

1. It is invalid

2. Censorship

Critically, the miner is tipped off that they should reconnect to a different pool or solo mine if an error is received but the block they proposed was valid. Thus, **Job Negotiation does not give miners the ability to work on any random block template they want, but it serves as an early warning system that alerts miners to possible issues with pool operators much earlier than if the miner was not running a full node and proposing their own work.**

EXAMPLE OF JOB NEGOTIATION IN ACTION

With this overview of how Job Negotiation works, we can now think about how it might actually come into play in the real world.

Let's suppose that 4 pools with a combined majority of the total network hashrate are all simultaneously commandeered by a malicious party (e.g., their nation's government). Despite the pool operators not wanting to tarnish their reputations or damage the network they have

a large stake in, the malicious party gives them no other choice but to participate in a 51% attack and deep reorg.
In the Stratum V1-only scenario, the miners supplying the actual hashrate to those pools might not realize that they are unwillingly participating in an attack until it's too late.

For a hypothetical future scenario in which some of those miners are choosing their own work, they would know that something is off as soon as their valid block templates were rejected. If miners controlling a large enough portion of the hashrate for those 4 pools were proposing their own work, they could effectively prevent a sustained 51% attack by switching pools as soon as their original pools start censoring them. It doesn't mean that all miners in those pools need to be proposing their own blocks — just a large enough percentage to bring the cumulative hashrate of the attacking pools below 50% if those miners running full nodes switch.

A quantity of 4 pools is used for this example because that is the minimum it would take with today's hashrate distribution, but it could just as well work with 1 pool having a majority of the hashrate in the future. It's important that some pools remain honest and uncompromised in this scenario, as solo mining isn't economically viable for the majority of miners.

WHAT ABOUT PAYOUTS?

Since pools are temporary custodians of mining payouts, one can argue that pools could simply not send BTC to a miner who, for example, includes a transaction in their block that the pool didn't want included. In other words, the pool can still censor their miners by attaching conditions to payouts, thus defeating the purpose of decentralized work selection. For this argument, there are two key points to consider:

- The pool either rejects or accepts block templates at the beginning of mining rounds, and the miner can propagate found blocks themselves.

67

- Pools send payouts frequently (multiple times per day in most cases), so the financial risk for miners of not getting paid for valid work is minimal. Meanwhile, pools who don't pay their miners risk permanent reputational damage and loss of future business.

As with many aspects of the Bitcoin ecosystem, there is a tradeoff between user experience and security. Large mining pools with thousands of users are not completely trustless, but offering frequent payouts and having adequate skin in the game minimizes risk, as does the easiness of switching pools at any time should trust be damaged.

DECENTRALIZATION FOR DECENTRALIZATION'S SAKE

Although we know how Stratum V2 Job Negotiation can be implemented practically, there's still a valid question as to whether or not today's miners care about building their own block templates. Stratum V2 improving Bitcoin's decentralization depends on Job Negotiation reaching significant adoption, and that may not happen. We can imagine some use cases emerging for Job Negotiation which incentivize its adoption, including the one we described above in which miners having well-connected nodes are able to increase their revenue by working on higher value blocks. Ultimately, we believe that this is a natural part of the evolution of the mining industry. Large scale miners are investing millions of dollars into building and maintaining efficient operations, and it takes a lot of time to break even on those investments. By running their own full nodes and working on their own block templates, miners can add redundancy (safety) to the network and strengthen Bitcoin's fundamentals at minimal added cost. That is in the self-interest of every miner wanting to protect and maximize their long-term ROI.

CONCLUSION

Decoupling block building and propagation from pool reward payouts is not a perfect solution, but it does provide an early detection system for malicious behavior by pool operators. It also adds more mining full nodes to the network and even incentivizes them to be well connected so that they can mine more valuable blocks with higher cumulative transaction fees. Adoption will not happen overnight, and in fact it may take many years. Nonetheless, we as pool operators are committed to building a full implementation of Stratum V2, offering Job Negotiation to our miners, and educating the community about this important and often misunderstood sector of the Bitcoin ecosystem. We hope that other pool operators will join us in this worthwhile initiative.

GO READ MORE:

Why Pools Mine Empty Blocks and How Stratum V2 Fixes This
Empty block mining is getting less common, but technical limitations are preventing it from going away completely. Enter Stratum V2.

Extending Mining ASIC Lifespans with Firmware
Understanding why custom firmware is one of the most important tools available to miners for improving the productivity and lifespan on ASIC mining machines.

Developing BOSminer: An Open-Source Replacement for CGminer
Background, timeline, and why we chose to build BOSminer in Rust.

MINING BUSINESS

There is much, much more to mining profitability than just finding cheap electricity. The thing is, all of that "much more" stuff comes after the "finding cheap electricity" part.

In the current halving epoch (following Block #630,000), we've seen the beginnings of an inevitable merge between the energy sector and bitcoin mining. A wide range of professionals with expertise in different areas—from oil and gas fields, solar and wind farms, hydro dams, nuclear reactors and even grid operators—are getting orange pilled through mining. And it all comes down to the simple fact that miners need cheap electricity to compete. With just this knowledge, some low time preference, and a basic understanding of the law of supply and demand, all the energy FUD could be dismissed and concerned environmentalists could turn their attention towards bigger issues.

Alas, these things take time. While we wait for more people to catch on and realize what's happening, the information asymmetry presents an opportunity. Those who source (or perhaps build) cheap energy sources and dive deep down the bitcoin mining rabbit hole can still prosper in the Satoshi Rush.

This section serves as a starter for going down the mining economics rabbit hole. We explain different strategies to succeed in the mining industry, how to calculate mining profitability projections, and some of the technologies like heat capture and recycling as well as immersion cooling that can give miners an edge.

Bitcoin Mining Profiles: The Investor, The Entrepreneur, and The Prospector

Categorizing the different Bitcoin mining strategies used to maximize profitability at any scale of operation.

Bitcoin's mining contest is an elaborate dance performed on the global stage of energy and capital markets, requiring significant expertise in the areas of industrial power, information technology, and capital investment. At its base level, however, bitcoin mining is just a service for hire, that offers security to the bitcoin network, for a price. This quick article is concerned with the dance, in finding the balance between these diverse, but not independent considerations. Under examination, we see that, among users who operate their own mining hardware, a few distinctive profiles emerge, based on the balance of these competing demands.

OPTIMIZE ASIC PERFORMANCE FOR MAXIMUM HASHRATE OR EFFICIENCY

It is reasonably well known that there is a trade-off between a bitcoin miner's (ASIC) efficiency, and its productivity. Typically, lower power modes permit higher efficiency (in TH/J; conversely a lower exhaust rate in J/TH), and higher power modes provide greater yields (measured in hashrate, TH/s) which means more BTC mined in a given time period. A crude plot depicting this idea follows:

Let us acknowledge that there are the two extremes of most interest:

1. Where the unit is most efficient (lowest J/TH), and

2. Where the unit is most productive (highest TH/s,)

While we observe that these operating points may be fluid, subject to change based on bitcoin's price and market conditions, it still remains that since mining is capital intensive and requires planning, a miner cannot deviate too far from their overall strategy without harming their investment.

CATEGORIZING BITCOIN MINING STRATEGIES

Based on my own experience with bitcoin mining, and my observation of others, this "efficiency continuum" informs the decisions of miners, who can be grossly generalized by the following three archetypes:

1. The Investor

2. The Entrepreneur

3. The Prospector

I'll spend the next few lines explaining each of these profiles. By identifying how you fit within the ecosystem of miners, you may find a greater chance of sustained profitability. The obvious caveat is that if you already have a professional mining operation, you have already developed your own mining style, and probably don't need to read this article. Regardless, the exercise may be instructive to those miners with less experience.

1. The Investor: professional groups led by visionary technologists and investors with deep pockets. They are on the bloody edge of technology, leaders of the mining arms race, locking up 100T+, S19-class machines. Their strategy depends on large-scale deployment and capital investment, which requires them to have their foot on the gas at all times. Due to the aggressive financial position, shipping delays, and machine downtime are a disaster. Plant availability (uptime) and warranty are critical for protecting the investment. Efficiency is less of an issue since they are the most capable of securing attractive bulk electricity pricing through creative agreements, or energy technology.

72

The Investor is the one driving the difficulty adjustment upwards, in an effort to dominate total hashpower, and to outpace and drive out their competitors. In all, the Investor is concerned with the highest productivity, which is accomplished through a combination of owning the "best" assets, and operational excellence.

2. The Entrepreneur: This is the scrappy startup, quintessential doers who can just make things work, through ingenuity and elbow grease. Since such an operation is usually the brainchild of one, or just a few wily individuals, they have more leeway to be creative, or explore unique or unconventional methods of production. They are probably most likely to find clever solutions that prove profitable. They probably quickly moved on from running factory firmware. They have to be more efficiency-minded than the Investor, because it's unlikely they will get more competitive energy pricing. With a strong internal engineering and operations capability, the Entrepreneur may be able to greatly reduce their capital expenditure, and for that reason be able to operate machines profitably, albeit under less ideal conditions.

3. The Prospector: This class of miner is most akin to individuals panning for [digital] gold. Just a blip on the hashpower radar, but they're out there, staking their claim (using proof of work; proof of stake is lame). These individuals are probably the most varied in composition. They are unilaterally nerds, and may also be makers, engineers, crypto-libertarians, or just hustlers trying to make a buck. Their motives are equally diverse: pure profit, procuring clean sats, learning about bitcoin, or breathing life into junker ASICs that they bought online. They are not encumbered by commercial agreements, and are most free to use the hardware as they wish. Many will not be able to earn coins profitably. They are the most sensitive to miner efficiency, since retail electricity rates will make it very hard, or impossible to earn a profit. For this reason, they will probably learn to run their miners at lower power, and seek more efficient operating points. For them aftermarket firmware is essential, in order to narrowly tune and optimize their miners. And since their profit margins are

razor thin, one must be extremely cautious not to overpay for their equipment, or the payback period will never be realized.

I'll be the first to admit that this is not a definitive list, but should still help inform the reader as they consider their own unique mining style. By comparing yourself to the profiles listed above, acknowledging the specific or unique advantages that you may have, and identifying where on the power-efficiency spectrum you fall, you will have a better understanding of the mining strategy that is most likely to serve you well. Thanks for reading, and *merry* hashing.

How to Calculate Bitcoin Mining Profitability

Methodology for calculating the expected profitability of mining bitcoin can be complex and involved. This article breaks down all the factors that affect profit.

Calculating potential Bitcoin mining profitability can be complicated. Deriving a precise number of expected mining revenue and profit requires more data inputs than most people realize. And correct estimations are essential to successful mining at any scale, small or large.

The Braiins mining profitability calculator is designed to support all the necessary inputs for accurate revenue determinations, but for some miners, managing almost two dozen different data fields can be overwhelming especially if it's the first time a miner is sitting down to run the numbers on their current or future operations.

This article is written as a companion resource to the profitability calculator. Each of the data points available on the Braiins calculator are explained so miners understand what they represent, how to find the data needed for each field, and how to correctly calculate their own mining profit projections.

Profitability Calculator on Braiins Insights

TIME

One of the first and most simple inputs is the timeframe for measuring revenue and profitability. The idea that Bitcoin incentives long-term planning is especially true in mining. Focusing on longer time periods is a more common strategy instead of mining with very short-term profit expectations. Set the range on the Braiins calculator for whatever timeframe is appropriate, between 6 and 60 months.

76

BITCOIN PRICE

This metric is also simple and easy to enter. Input the current bitcoin price based on the number displayed by whatever exchange a miner prefers to use or a data aggregator like OnChainFX. Expected future changes in bitcoin's price are input in another field explained later in this post.

NETWORK DIFFICULTY

Input the current network difficulty level to this field. Expected future changes in bitcoin's mining difficulty are input in another field explained later in this post.

See current difficulty level on the Mining Insights dashboard.

HASHRATE

Hashrate is a value derived from the estimated amount of hashes being generated to solve new blocks. Every make and model of mining hardware has a factory estimated hashrate in the product details. Hashrate is generally measured in terahashes per second (TH/s). Find the hashrate for whatever machines are (or will be) operational, and sum the total hashrate for all operational machines. Enter the value in the Hashrate field.

See historical hashrate data on the Mining Insights dashboard.

CONSUMPTION

Power consumption is one of the most important data inputs for any mining operation's profit calculations, and unlike other data, it's relatively easy to predict although it's not a fixed number. Miners usually measure their power consumption in watts (W) per hour (W/h) or kilowatt hours (kWh). One kW equals 1,000 W. Every bitcoin

mining machine specifies its factory estimated power consumption
in the product details, but the real number can fluctuate. Through
normal use, power consumption can increase slightly over time or it
can change significantly bychoice of the operator when using tools
like Braiins OS+ firmware.

Find a machine's estimated power consumption in the product details
and, for miners operating more than one machine, simply sum the total
expected consumption for all operational machines and, if appropriate,
account for increases from overclocking with custom firmware.

ELECTRICITY PRICE

The cost of power is one of the data points miners care about most,
and electricity prices can vary significantly across different geographic
regions. Prices can also vary over time unless a miner secures a
power purchase agreement with future power price predictability.
Even without that agreement in place, for the purposes of estimating
future revenue, a miner can generally use their current power price
for future projects. Consider also slightly adjusting power prices up
and down to see its effects on future profit.

BLOCK SUBSIDY

The number of new bitcoins created when each block is mined is
the block subsidy. This number changes after each halving event,
which takes place once every four calendar years, approximately. For
most revenue calculations, adjust the block subsidy if the model is
extended beyond the date of the next halving. Otherwise the current
block subsidy can be used.

POOL FEE

Fees can vary significantly across different pools, but rarely do pool fees rarely change, or at least change significantly. Compare fees across different pools by substituting them into the Pool Fee field and see the effect on long-term profitability.

AVERAGE TRANSACTIONS FEES

The block subsidy is only one part of the full block reward paid to miners who win each block.
Transaction fees for spends included in the block are also paid. Like price and hashrate, transaction fees paid per block vary significantly over time as network use and spend sizes vary.

See average fees per block for the past 2016 blocks (14 days) on the Clark Moody Dashboard.

OTHER FEES

Additional costs for custom firmware, hosting services, management fees, revenue sharing, or other operational expenses should be summed and entered into the Other Fees field.

DIFFICULTY INCREMENT

Percentage increases of difficulty per year should be entered here.

Difficulty determines how much computing power is required to mine new blocks. Changes in difficulty levels result in changes for how many hashes must be statistically generated to find a valid Bitcoin block. Higher difficulty means more computing power which ultimately means more power consumed by miners, increasing operational costs. Difficulty is measured in arbitrary "difficulty units," meaning the number is relative. When attempting to accurately estimate

79

revenue, understanding the long-term trajectory of mining difficulty is essential.

Each year difficulty changes approximately 24 times (twice per month), so the percentage increase would reflect the total change from the first adjustment to the last over that period. For example, the average increase of mining difficulty over the past 5 years is 6% monthly, which equates to roughly 100% per year.

PRICE INCREMENT

Like Difficulty Increment, this field should contain the expected annual increase for bitcoin's price. Bitcoin's price is difficult to predict, so consider different bullish and bearish scenarios with the number entered into the calculator price field. Modeling profit with different price levels over long periods of time helps miners to better understand different ranges of profitability. Miners can also use long term price averages to calibrate their expectations of revenue and profit using more general historical price tools (e.g., 200-day moving average).

Profitability Calculator on Braiins Insights

CAPITAL EXPENDITURES (CAPEX)

Capital expenditures are funds spent by an entity to purchase, replace, upgrade, or otherwise manage physical assets (e.g., mining machines, facilities). Common CapEx fund uses can vary significantly in type and amount across different mining operations, but common expenditures in mining include:

- Buying ASICs and PSUs;

- Constructing, remodeling, or maintaining a mining facility;

- Cooling equipment (e.g., HVAC or immersion tanks);

- Compliance costs.

Sum these costs and enter the final number denominated in dollars in the CapEx field. And even if a complete CapEx cost analysis isn't available, estimates are still valuable for modeling the effect of expected expenditures on long-term mining revenues.

MONTHLY OPERATING EXPENSES (OPEX)

Operating expenses are typically recurring or cyclical costs independent from mining revenue that maintain the operation. Since electricity costs are already entered in an earlier field, the sum of expected monthly OpEx does not include power costs for miners in the Braiins calculator. Examples of common OpEx funds for miners include:

- Salaries

- Site Security

- Insurance

- Taxes and legal fees

81

INITIAL HARDWARE VALUE

The data input for the value of mining hardware field comes from simply summing the total purchase price of hardware purchased, or in the case of a miner that has not yet bought machines, estimate the current market value of mining hardware based on the prices listed by manufacturers or hardware resellers.

HARDWARE APPRECIATION OR DEPRECIATION

This input represents the annual percentage change in the value of a miner's infrastructure. The value of physical assets like mining machines changes over time, and appropriately depreciating hardware over time – especially as newer and more efficient models enter the market – is an essential calculation for any mining operation, regardless of size. Talk with a tax consultant to understand more details about how to accurately depreciate hardware.

INITIAL INFRASTRUCTURE VALUE

Besides the mining machines, a mining operation also includes a variety of other valuable assets, including land, containers, buildings, cooling equipment, and more. Enter the dollar-denominated value of these assets excluding the value of the actual mining hardware.

HODL RATIO

This input is one of the most important advanced options because it represents how much of the newly mined bitcoins a miner plans to hold. Most miners sell some portion of their revenue to cover operating costs. But it's common to hold some portion of mined Bitcoin on their balance sheet, giving them exposure to potential price appreciation. HODL ratio is directly dependent on the price increment factor and impacts long-term profits as the price of bitcoin fluctuates. Enter the expected HODL ratio as a percentage. For example, a miner

82

that does not sell any bitcoins has a HODL ratio of 100%. A miner that sells most of their bitcoins could have a HODL ratio of 25%.

DISCOUNT RATE

The discount rate is an interest rate used to determine the present value of future cash flows. This helps determine if future cash flow from a mining operation will be worth more than the capital spent to fund the operation now. A non-zero discount rate will not impact the data series visualized on the mining calculator, but the calculator's backend calculates Net Present Value (NPV) and includes this value in the CSV file download.

WHAT IF SOME DATA IS MISSING?

A useful mining revenue model doesn't have to include data for every input described above. But mining operations that are missing several inputs should consider why chunks of data are missing, since most of the fields represent information that should be readily available to most miners.

Still, models are estimates and will not be severely impacted by entering roughly calculations or estimated inputs. After all, every miner produces bitcoin at slightly different costs across a host of variables. Apply common sense and careful estimations, and the resulting revenue model should be sufficiently reliable to guide a mining operation's future planning.

Final thought: There's no fixed cost for mining bitcoin. The real cost for each miner depends on over a dozen variable data points.

Green Innovation in Bitcoin Mining: Recycling ASIC Heat

Highlighting lower-carbon use cases for Bitcoin mining and why cleantech will play a role in the next evolution of the mining sector.

This article was written in collaboration with Magdalena Gronowska, a Bitcoiner who has 10 years of experience in energy and carbon markets.

Bitcoin mining is an energy intensive industry. Correspondingly, miners exude large quantities of heat as a byproduct of the hashing process, which conventionally has been vented into the atmosphere. Competitive mining companies are exploring different ways to recover and repurpose waste heat to create additional revenue streams and offset electricity costs.

Heat recovery is a low-carbon technology that cuts across multiple sectors of the economy. Low-grade heat — i.e. low-temperature heat expelled by miners — is required to heat homes and buildings and by certain manufacturing processes (such as in food and beverage production or pulp and paper manufacturing). The primary challenges are identifying effective ways to capture and transfer heat, along with sound economic use cases.

The re-use of waste heat offers environmental benefits — **it offsets energy consumption and any associated carbon emissions.** Even larger environmental benefits occur if clean electricity powering miners displaces heat generated from fossil fuels. Historically for example, coal, bunker fuel, propane, or natural gas have been used by the North American agricultural industry in heating systems.

84

Heat recovery applications are a compelling use case for Bitcoin mining in that they can be implemented within both centralized and decentralized mining applications. A large-scale mining installation coupled to a large heat load like a manufacturer, greenhouse, or district heating system could economically benefit in the same way that smaller distributed miners could provide space and water heating for residential and commercial uses.

Energy consumption represents the largest operating cost for mining operations (79% of operational expenses on average). This makes bitcoin mining one of the most energy price-sensitive industries in the world.

Large-scale mining facilities exist in the US, Canada, Iceland, China, Russia, Kazakhstan, Georgia, and Russia, their specific locations largely determined by the holy grail of the mining industry: **low electricity prices.** A few particularly innovative miners, however, have found a way to share their power bills with other seemingly unrelated businesses.

In this article, we examine 5 mining projects that are helping reduce greenhouse gas emissions by repurposing the heat produced by their ASICs. These projects are important milestones for establishing the feasibility and economics of green Bitcoin mining.

CANADA — MINTGREEN

Bitcoin mining is literally boiling the ocean in an innovative heat recovery application on Vancouver Island, Canada. But this is far from the environmental disaster denounced by Bitcoin's detractors — it's the next generation of green mining technology.

The key to MintGreen's sustainable mining model is that energy is used twice; first to mine Bitcoin, and then to provide zero carbon industrial heating. These systems generate persistent and predictable heat loads year-round, which are sold via heat offtake agreements.

85

MintGreen's commercial partnership with Vancouver Island Sea Salt uses a liquid immersion mining system to heat large evaporation tanks to produce gourmet flake salt. Their second collocated site at the Shelter Point Distillery, uses heat from mining in the mash process to make whisky. Salt and whisky – a killer combination for any crypto carnivore.

SWEDEN — GENESIS MINING GREENHOUSES

This pilot project gives a new meaning to "green" Bitcoin mining. Genesis Mining has partnered with a handful of public and private organizations in Sweden to develop mining containers with specialized air flow systems that direct waste heat flow into a nearby greenhouse that grows fruits and vegetables. Researchers predict that if a 600kW Genesis mining container can increase greenhouse temperatures by just 20 degrees, the size of the greenhouse can triple in subarctic climates.

„A 1 MW data center would have the ability to strengthen the local self-sufficiency up to 8% with products that are competitive on the market."

- Mattias Vesterlund, Senior Researcher at RISE (Research Institutes of Sweden)

While the project is still in its early stages, Genesis plans to scale this to their other mining operations around the world in the future, most of which are powered by renewable energy. This use case can be replicated by other miners across a variety of farm crops — from fruits and vegetables, to aquaculture, insects, and algae farming.

NETHERLANDS — GREENMINE CONTAINER

Multiple industrial symbiosis projects between miners and greenhouses are being explored in Europe. In the Netherlands, a greenhouse tomato farm is co-locating with a liquid immersion cooled mining container. This GreenMine Container mines cryptocurrencies

86

and pipes the heat output into an adjacent greenhouse. The heat from the miners is efficiently removed using a non-corrosive oil, transmitted through a heat exchanger, and converted into hot water that heats the greenhouse.

A key feature to note is that this type of solution is extremely scalable. The containers are prefabricated in a standardized way and can be easily transported and installed next to greenhouses, commercial buildings, or any other facilities that require low-grade heat. As enterprise-scale mining operations grow more common, smaller-scale mining operators are at a competitive disadvantage because they cannot leverage economies of scale. Modular and mobile mining containers enable smaller operators to more effectively compete with large players by improving their economic viability through co-locating with heat loads.

SUSTAINABLE MINING AND FOOD PRODUCTION: AN ENGINEERING MATCH MADE IN HEAVEN

Building out mining capacity around the world has broader implications beyond increasing domestic manufacturing capacity. Similar to how mining can improve the economics of renewables and other energy infrastructure where it is currently not feasible, such as to grid disconnected communities or stranded energy resources, mining can also improve the economics of food production.

Reusing waste heat for food production can offer broader societal benefits — it can help address domestic food insecurity and unreliability. Food insecurity is disproportionately worse in Northern regions, like Canada and Alaska, where the majority of fruits and vegetables are imported, resulting in lower nutritional value and increased food spoilage.

 Co-locating miners with food producers can improve the economics of providing fresh food year-round. In addition to large-scale

87

greenhouse operations highlighted in the two examples above, shipping container farming using hydroponics (a farming technique that grows plants in a solution of water and nutrients without any soil) are well-suited to more remote or distributed containerized mining farms as these systems are equally modular, mobile, and stackable. Governments often subsidize access to nutritious food for their citizens; however, there is an economic case to be made for targeting more sustainable and self-sufficient methods of food production instead of perpetual subsidies. Forward thinking countries like Sweden are recognizing the opportunities to achieve industrial synergies between two very different industries.

FRANCE — SATO FROM WISEMINING

Just announced earlier this February, WiseMining is an early-stage project from WisElement, which is a French startup working on building solutions to reduce the energy consumption of buildings. WiseMining has developed a Bitcoin water boiler where the ASIC hashboards (containing the chips that do the actual mining hash computations) are removed from their typical metal "shoebox" and placed directly into a custom container below the water boiler. This type of setup has numerous advantages, which are explained more in the next section.

The idea for a boiler that uses ASICs for heat production has been around for many years and is rather simple in theory, but it has proven difficult to put into practice so far. Adding mining hardware and supplementary components to a boiler system increases the up-front costs compared to a traditional water heater, as well as potentially adding extra complexity to operating and maintaining it.

Based on WiseMining's prototype for Sato, we think the potential is there for this application to be viable. Regardless, for some Bitcoiners, the opportunity to heat their home with miners may be worth the additional costs, even if the mining revenue does not fully recover the initial capital investment.

UNITED STATES — SPA-256 HOT TUB

This article simply wouldn't be complete without the fun use case that originally inspired it: the SPA-256 by Jesse Peltan.

Jesse arranged his ASICs in an oil bath, similarly to the hashboards in the WiseMining prototype, MintGreen's pilot projects,or the GreenMine Container. The heat absorbed by the fluid is transferred to a liquid-to-liquid heat exchanger, which can be used to heat the spa.

Immersion cooling offers several key benefits:

- The ASICs run more efficiently than if they are air cooled, as there is no need to run fans to blow out the hot air.

- There is a much lower risk of overheating, so the ASICs can be more safely overclocked to increase hashrate.

- Immersion cooling has the potential to extend the lifespan of the silicon hashing chips as it cools them more effectively.

- While ASICs are normally very loud, they are practically silent when immersed.

Cooling fluid has far greater heat density (>1000x) than that of air, which means that it can safely absorb a lot more heat output from the ASICs and transfer it more effectively through a heat exchanger. This is some seriously cool engineering and probably the most relaxing method of stacking sats we have ever seen.

THE NEXT GENERATION OF GREEN MINING

The innovative use cases for repurposing heat that we have described in this article are just one of many ways that Bitcoin's environmental
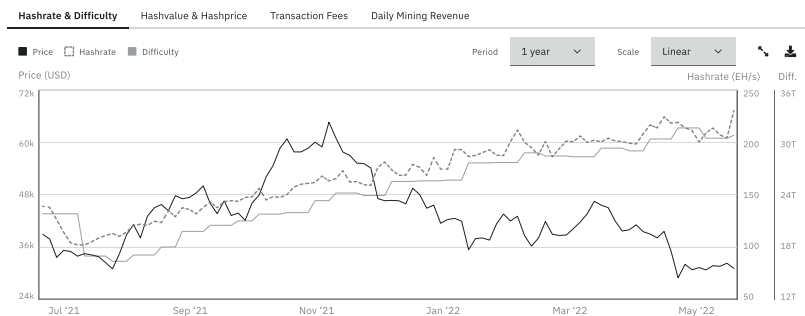
impact can be lowered. What's particularly exciting is that these applications are in the economic self-interest of miners, as they convert what would otherwise be a waste product (heat) into something useful. As the mining industry continues to evolve and optimize, we expect innovative heat recovery applications, as those featured above, to become more commonplace — and especially when the large profit margins that miners enjoy during this bull market inevitably shrink and competition grows fiercer.

Carbon pricing and complementary policies advancing heat recovery and district heating initiatives will further incentivize miners to "dabble" in cleantech. Many countries provide considerable public sector funding for low-carbon or energy efficiency equipment in manufacturing or the agricultural sector. I see a future phase of pilot projects in the Bitcoin mining sector exploring fully integrated systems where heat and carbon dioxide and other air emissions from fuel combustion will be recovered to produce food, pharmaceuticals, or purpose grown biomass for biofuels, as are currently being piloted in the power generation industry. Savvy companies will take advantage of millions of dollars in government funding to optimize for multiple revenue streams.

90

Economics of Immersion Cooling for Bitcoin Miners

An analysis of the big question: "Is immersion cooling worth it?" with long-term profitability projections for Antminer X19s in immersion with Braiins OS+

The day is June 18th, 2021. China is extending its provincial cryptocurrency mining ban in Xinjiang and Inner Mongolia to be nationwide, just as the ultra-profitable rainy season in hydropower-dense Sichuan province is getting going. Network hashrate — once practically a sure bet to exceed 200 EH/s by mid-year — now drops back below 100 EH in July. The miners who have hash online in the summer of '21 see their revenue temporarily double in bitcoin terms, from under 500 satoshis/TH/day to nearly 1000 sats/TH/day.

Hashrate and difficulty charts on insights.braiins.com

Fast forward to late May, 2022. Resilient miners in China have gotten smarter about their network infrastructure and security so that they can continue hashing away, although not nearly at the same scale as before. While some employees of a leading Chinese hardware

91

manufacturer have suggested in friendly conversations that as much as 30-40% of network hashrate remains in China today, this author (with almost no contacts in China) believes it's more likely below 20%.

Meanwhile, the 30-day moving average for total network hashrate has been sitting above 200 EH/s for a couple weeks now. As for where the new hashrate is coming online, there is simply no debate. North America has picked up China's slack and then some, with Texas becoming the clear global frontrunner in terms of hashrate m^2 (even though Texas is huuuuuge). With this hashrate migration to North America and Texas in particular, we are in for an interesting summer. West Texas, the home of much intermittent solar and wind energy, is about to get hot. Like, swelteringly hot.

This presents a problem for bitcoin miners. When it's really hot outside, mining hardware runs less efficiently and with a greater risk of failure. The consequences can cause downtime and loss of revenue due to machines automatically turning off once temperature readings reach dangerous levels. Additionally, it can lead to fried hashboards and other permanent hardware damage if the machines don't shut down in time. (Braiins OS+ Dynamic Power Scaling feature fixes this.)

To make matters worse, the most popular ASIC hardware family today is the Antminer X19, which is extremely sensitive to heat relative to older miners like the S9 and Whatsminer M20S. As we've described in our research summary, the power consumption of Antminer X19 models can increase by 40%+ with higher temperatures even as frequencies are constant, meaning that the J/TH efficiency of the machines suffers significantly. It's no surprise then, that public miners such as Riot and Argo are building exclusively immersion cooling infrastructure for their new miners coming online in Texas. Immersion cooling alleviates the majority of the temperature impact on mining operations. Rather than worrying about your mining fleet's uptime, power consumption, and lifespan, you can respond to temperature rises by increasing pump speeds and running dry coolers / cooling

towers harder, keeping your total hashrate and power consumption much stabler and decreasing operational risks. For well-capitalized miners operating in hot climates, it just makes sense.

But what about for the pleb miners with a machine or two or five at home? What about the miners with 1-6 MW operations in Paraguay or Mexico? Hell, what about the miners in Wyoming, Montana, and the Dakotas where it's very cold for a good portion of the year but those few summer months can see temperatures exceed 100F (38˚C) on rare occasions? Does it make sense for any of those miners to invest in immersion cooling? Well, let's find out.

BENEFITS OF IMMERSION COOLING FOR BITCOIN MINERS

Before getting into the economic analysis, it's important to understand the advantages of immersion compared to air cooling that help justify its higher up-front cost. To briefly summarize, immersion cooling offers the following benefits:

- **More effective heat dissipation:** the fluids used in immersion, called dielectric coolants, are much more thermally conductive and dense than air, making them better at absorbing heat and moving it quickly away from the miners.

- **Increased hardware lifespan:** small vibrations and rapid temperature fluctuations degrade hardware lifespan and immersion cooling greatly reduces both of these because the fluid temperature is more stable than air and the fans, which produce the vibrations in air, can be removed in immersion.

- **Better operating conditions:** the immersion fluid prevents dust and debris from getting into the hardware, decreasing

cleaning and maintenance requirements. Also, the removal
of the fans and density of the fluid practically eliminates
the noise which can be deafening for miners in air.

- **Improved Efficiency (J/TH):** on a new-generation miner
  like an Antminer S19, the 4 fans consume roughly 35 W
  each, accounting for ~5% of the machine's total electricity
  consumption in air. Removing them to run in immersion
  means that the 5% energy savings can go towards more
  hashing, improving the J/TH by roughly that amount.

- **Safer Overclocking (more TH/s):** the more effective
  heat dissipation and operating conditions in immersion
  also enable miners to overclock their machines to a very
  significant degree, as we'll see later in this article.

All of these benefits make immersion cooling superior to air
cooling regardless of the climate that the miner is operating in.
However, it comes at a much higher up-front cost, so there's
still a question of whether or not immersion cooling is worth
it. While that will depend largely on the local climate of the
operation, this article will outline the structure for making this
determination with all of the not-so-small details to consider with it.

MINING INFRASTRUCTURE CAPEX: IMMERSION VS. AIR COOLING

As is the case with all future profitability calculations we do for
bitcoin miners, we're going to have to make a lot of assumptions and
generalizations here in order to get anywhere.

Honing in on a narrow price range for building mining infrastructure
just isn't possible. It depends on all sorts of factors that change over
time and across different locations, as well as with the size of the
operation being built. For example, labor in Paraguay and Mexico is

relatively cheap compared to the US and Canada. On the other hand, many of the parts required for infrastructure would need to be shipped internationally, which may also include extra import costs. And modular, mobile infrastructure (i.e. mining containers) will generally cost more per MegaWatt than large static facilities that can host 10+ MW worth of miners.

So, let's simplify matters and just lay out some assumptions. **Building air cooled infrastructure can cost anywhere from $150-400k/MW, depending on everything described above.** Some portion of that cost is for cooling, including wet curtains and industrial-sized intake and exhaust fans, as well as insulative material to separate hot and cold aisles. All together, those components will rarely account for more than 10% of total infrastructure CapEx, while the more common case is probably at or below 5%. Meanwhile, the lion's share of the costs will be from labor, materials, and electrical equipment and wiring.

Immersion mining infrastructure will still have nearly all the same costs as air cooled, minus about 5% ($7.5k-20k/MW) for the cooling components that are no longer needed. However, immersion will add all sorts of new and costly components to the infrastructure:

- Dry coolers / cooling towers

- Tanks and frames

- Pumps and pipes

- Heat exchangers

- Dielectric coolant

- Sensors and monitoring / control systems

After analyzing dozens of different immersion systems varying in size from small DIY tanks with 2-4 mining machines to industrial-scale facilities, we've found that the extra CapEx for building immersion infrastructure is almost identical to the original air cooling CapEx

95

range, $150k-350k per MegaWatt, not including shipping costs. This means that the total cost for immersion infrastructure should be somewhere in the wide range of $280k-730k/MW, although the upper portions of both the air cooled and immersion ranges are generally for modular containers which wouldn't be combined with each other. More realistically, then, **let's say that the total immersion cost should be somewhere in the $280-600k range.**

Now, all that's left to do is answer the question of whether that extra CapEx is worth it for all the benefits immersion provides.

This article contains many charts from our profitability calculator that are extremely data-dense and would be difficult to read in black and white. If you'd like to read the rest, you can find it on the Braiins blog by scanning the QR code below.

GO READ MORE:

Bear Market Mining (Part 1): Setting Expectations
Thinking through the metrics that matter for miners and how to set expectations and operational boundaries to avoid panic in the future.

Economics of Bitcoin Mining with Solar Energy
An economic analysis of bitcoin mining when using an intermittent, renewable energy source like solar power.

Optimizations for Bitcoin Mining with Intermittent Energy Sources
Exploring methods to reduce capital expenditures (CapEx) and operational expenditures (OpEx) as well as improve ASIC hardware lifespan for bitcoin miners with intermittent power supplies.

97

MINING MEMES

Memes are the message. Any narrative will inevitably bend toward memes that zing, and nowhere is this truer than in the bitcoin mining sector. Create good memes, and the narratives will follow.

What is a meme? This internet-native social phenomenon is a communication tool that can embody almost any form of multimedia to distill and distribute an idea. Most meme artists intent to elicit humor from viewers while simultaneously communicating their feelings and opinions about any given social, economic, or political issue.

Bitcoin is also an internet-native social phenomenon, so it's no surprise that memes play an enormous role in the formation and propagation of many ideas around the world's largest cryptocurrency. Especially for the bitcoin mining sector, important conversations around topics like computing hardware, electrical grid infrastructure, power consumption, stranded energy and more. If pictures are worth 1,000 words, an effective meme is worth 10,000.

This section is dedicated to showcasing a sample of some exquisite, evergreen mining memes created by various entities in the bitcoin mining community along with brief explanations for why each meme matters.

THE MINING MEMES

Resilience and self-sovereignty are essential values for miners, not just in the general bitcoin economy. Especially as any amount of energy consumption is criticized, as financial surveillance infrastructure expands, and the bitcoin economy truly becomes the only escape, at-home mining is an essential tool for protecting financial independence and self-sovereignty.

The urge to accumulate more mining hardware is often very strong, and few novice miners stop after just one machine. Because more hashrate means more bitcoin, the economics of stacking more hash make sense as a long-term investment or financial plan. A mining-centric version of popular meme format showing different preferences between the current generation and their parents illustrates this drive for more hashrate.

Sometimes the memes write themselves, and this is often true with mainstream media news coverage of the bitcoin mining sector. No additional artistry is required to produce a concise and easily comprehensible meme about perplexing news coverage. Side-by-side headlines on bitcoin's environmental effects before and after China's mining ban effectively demonstrate this type of meme.

Bitcoin miners are nothing if not self-aware, and all the idiosyncratic vernacular, odd habits, and nerdy behaviors are proudly embraced as signals of participating in building world-changing infrastructure.

THE BITCOIN MINEOOOOOR

101

Mining is certainly a more complex way of accumulating bitcoin compared to simply pressing a "buy" button on an exchange website. With the complexity, comes cheaper prices, higher long-term profitability, and other benefits. But the task of mining can be a handful, which is entertainingly represented below on a picture of American actor Ben Affleck.

Some of the best memes are as straightforward as they are corny. Taking a common meme format like the one shown below and replacing a couple words is an easy way to produce an instantly popular (even if slightly derivative) meme. (And who ever said brands like Braiins can't meme?)

Dad: Son, why are your eyes red?

Son: I smoke weed, Dad

Dad: Don't lie. You're crying because my hashrate is higher than yours with Braiins OS+

Other memes are meant to be used repetitively as an online conversation insert and a placeholder of sorts that reminds of recurring tropes and themes. One such example is questions from our beloved mining community about Braiins OS+ firmware for MicroBT machines, which, yes, is still being developed and is coming soon.

BY MINERS,
FOR MINERS

BRAIINS – BITCOIN MINING TOOLS

Optimizing mining operations with a full-stack
solution including ASIC autotuning firmware,
farm management tools, and the oldest
mining pool.

BRAIINS OS+   FARM Proxy

BRAIINS POOL

Formerly **Slush Pool**

INSIGHTS.BRAIINS.COM